Math 120A — Introduction to Group Theory

Neil Donaldson

Fall 2023

1 Introduction: what is abstract algebra and why study groups?

To be *abstract* means to remove context and application. A large part of modern mathematics involves studying patterns and symmetries (often those observed in the real world) from an abstract viewpoint so as to see commonalities between structures in seemingly distinct places.

One reason to study groups is that they are relatively simple: a *set* and a single *operation* which together satisfy a few basic properties. Indeed you've been using this structure almost since Kindergarten!

Example 1.1. The integers $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, 3, \ldots\}$ together with the operation $+$ is a group.

We'll see a formal definition shortly, at which point we'll be able to verify that $(\mathbb{Z}, +)$ really is a group. The simplicity of the group structure means that it is often used as a building block for more complicated structures.[1] Better reasons to study groups are their ubiquity and multitudinous applications. Here are just a few of the places where the language of group theory is essential.

Permutations The original use of *group* was to describe the ways in which a set could be *reordered*. Understanding permutations is of crucial importance to many areas of mathematics, particularly combinatorics, probability and *Galois Theory*: this last, the crown jewel of undergraduate algebra, develops a deep relationship between the solvability of a polynomial and the *permutation group* of its set of roots.

Geometry Figures in Euclidean geometry (e.g. triangles) are *congruent* if one may be transformed to the other by an element of the *Euclidean group* (*translations, rotations* & *reflections*). More general geometries are also be described by their groups of symmetries. Geometric properties may also be encoded by various groups: for example, the number of holes in an object (a sphere has none, a torus one, etc.) is related to the structure of its *fundamental group*.

Chemistry Group Theory may be applied to describe the symmetries of molecules and of crystalline substances.

Physics Materials science sees group theory similarly to chemistry. Modern theories of the nature of the universe and fundamental particles/forces (e.g. gauge/string theories) also rely heavily on groups.

Of course, the best reason to study groups is simply that they're *fun*!

[1] For example, $\mathbb{Z}$ together with the two basic operations of addition and multiplication is a *ring*, as you'll study in a future course.

Example 1.2. To introduce the idea of abstraction, we consider what an equilateral triangle and the set $\{1,2,3\}$ have in common.

The obvious answer is the number *three*, but we can say a lot more. Both objects have *symmetries*: rotations/reflections of the triangle and permutations of the set $\{1,2,3\}$. By considering *compositions* of these symmetries, we shall see that the sets of such are essentially identical.

Permutations of $\{1,2,3\}$ These can be written as functions using *cycle notation*.[2] For instance, the cycle $(1\,2)$ is the *function* which swaps 1 and 2 and leaves 3 alone, while $(1\,2\,3)$ permutes all three numbers:

$$(1\,2):\begin{cases}1\mapsto 2\\2\mapsto 1\\3\mapsto 3\end{cases}\qquad\text{and}\qquad(123):\begin{cases}1\mapsto 2\\2\mapsto 3\\3\mapsto 1\end{cases}$$

It is not hard to convince yourself that there are six distinct permutations of $\{1,2,3\}$; for brevity, we use the symbols $e,\mu_1,\mu_2,\mu_3,\rho_1,\rho_2$.

Identity: leave everything alone	Swap two numbers	Permute all three
$e=()$	$\mu_1=(2\,3)$	$\rho_1=(1\,2\,3)$
	$\mu_2=(1\,3)$	$\rho_2=(1\,3\,2)$
	$\mu_3=(1\,2)$	

Since the permutations are functions, we may compose them. For instance (remember to do ρ_2 first!),

$$\mu_1\circ\rho_2=(2\,3)(1\,3\,2):\begin{cases}1\mapsto 3\mapsto 2\\2\mapsto 1\mapsto 1\\3\mapsto 2\mapsto 3\end{cases}$$

The result is the same as that obtained by the permutation $(1\,2)=\mu_3$, whence we write

$$\color{red}{\mu_1}\circ\color{blue}{\rho_2}=\color{green}{\mu_3}$$

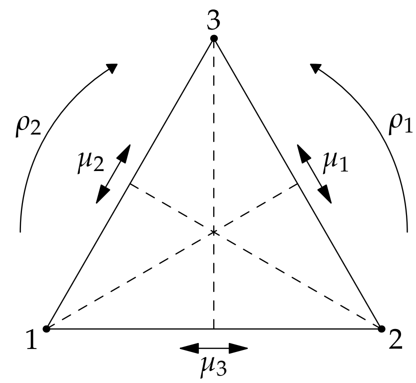
The full list of compositions may be assembled in a table; read the left column first, then the top row.

$\circ$	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	e	μ_3	μ_1	μ_2
ρ_2	ρ_2	e	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	e	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	e	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	e

[2]We will return to this notation in Chapter 5, so don't feel you have to be an expert now. The permutation (12) is known as a *2-cycle* because it permutes two objects. The permutation (123) is similarly a *3-cycle*.

The Equilateral Triangle What does all this have to do with a triangle?

If we label the vertices of an equilateral triangle 1,2,3, then the above permutations correspond to *symmetries* of the triangle: ρ_1 and ρ_2 are rotations, while each μ_i performs a reflection in the altitude through the i^{th} vertex.



The two sets of symmetries apply to different objects, but the structure of their *compositions* are identical.

What do we gain from this correspondence? Intuition, for one thing! There is a qualitative difference between the *rotations* ρ_1, ρ_2 and the *reflections* μ_1, μ_2, μ_3 of the triangle: since reflections flip the triangle upside down, it is completely obvious that composition of reflections produces a rotation! The corresponding idea that composition of 2-cycles makes a 3-cycle is not so clear.

Group theory, and abstract algebra more generally, is about ideas like this; by prioritizing abstract symmetries and patterns associated to objects over the objects themselves, unexpected connections are sometimes revealed.

Summary In this introductory example we considered two groups, which we now name:

> S_3 is the *symmetric group* on three letters (permutations of $\{1,2,3\}$)
>
> D_3 is the *dihedral group* of order six (symmetries of the equilateral triangle)

The formal way to say that the resulting group structures are identical is to call them *isomorphic*,[3] and we'll write $S_3 \cong D_3$.

As we progress, we'll see more examples of such relationships between seemingly different structures. In the first half of the course (Chapters 2–5) the primary goal is to become familiar with the most commonly encountered examples of groups so that they may quickly be recognized, even when well-disguised. The second half of the course is more abstract, with relatively few new examples of groups; comfort with the standard examples will be crucial in making sense of this harder material.

[3] We will explain the term *isomorphic* more concretely in Section 2.3 and revisit both examples in Chapter 5. For the present, observe the use of the congruence symbol $\cong$; given your understanding of congruent objects in geometry, think about why the use of this symbol isn't unreasonable.

2 Groups: Axioms and Basic Examples

In this chapter we define our main objects of study and introduce some of the common language that will be used throughout the course. Most of the examples are very simple and many should be familiar. We start by individually considering the axioms of a group.

2.1 The Axioms of a Group

Definition 2.1 (Closure). A *binary operation* $*$ on a set G is a function $* : G \times G \to G$. Equivalently,

$$\forall x, y \in G, \text{ we have } x * y \in G \tag{†}$$

We say that G is *closed* under $*$, and that $(G, *)$ is a *binary structure*.

In the abstract, including most theorems, we typically drop the symbol and use *juxtaposition* ($x * y = xy$). In explicit *examples* this might be a bad idea, say if $*$ is addition...

Examples 2.2. 1. Addition $(+)$ is a binary operation on the set of *integers* $\mathbb{Z}$: explicitly,

Given $x, y \in \mathbb{Z}$, we know that $x + y \in \mathbb{Z}$

This isn't a claim you can *prove* since it is really part of the definition of addition on the integers.

2. Subtraction $(-)$ is *not* a binary operation on the positive integers $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$. This you can prove; to show that (†) is *false*, simply exhibit a *counter-example*

$$1 - 7 = -6 \notin \mathbb{N} \qquad (\exists x, y \in \mathbb{N} \text{ such that } x - y \notin \mathbb{N})$$

On the integers, however, subtraction is a binary operation.

3. It can be convenient to use a table to represent a binary operation on a *small* set; for instance the example describes an operation on a set of three elements $\{e, a, b\}$. Read the *left* column first, then the *top* row; thus

$*$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	a

$$ab = e$$

We'll continue checking these examples for each of the group axioms.

Definition 2.3 (Associativity). A binary structure $(G, *)$ is *associative* if

$$\forall x, y, z \in G, \quad x(yz) = (xy)z$$

Associativity means that the expression xyz has unambiguous meaning, as does the usual *exponential/power* notation shorthand, e.g. $x^n = x \cdots x$.

Examples (ver. II). 1. Addition is associative: $x + (y + z) = (x + y) + z$ for any integers.

2. $(\mathbb{Z}, -)$ is non-associative: e.g. $(1 - 1) - 2 = -2 \neq 2 = 1 - (1 - 2)$.

3. $(\{e, a, b\}, *)$ is non-associative: e.g. $a(b^2) = a^2 = e \neq b = eb = (ab)b$.

Definition 2.4 (Identity). A binary structure $(G, *)$ has an *identity element* $e \in G$ if

$$\forall x \in G, \quad ex = xe = x$$

Examples (ver. III). 1. Addition has identity 0: that is $0 + x = x + 0 = x$ for any integer x.

2. $(\mathbb{Z}, -)$ does not have an identity: e.g. if $e - x = x$, then $e = -2x$ depends on x!
3. $(\{e, a, b\}, *)$ has identity e; observe the first row and column of the table.

By convention, if G is finite and has an identity (e.g. Example 3,) we list it first. Indeed, we can always list *it* first, since...

Lemma 2.5 (Uniqueness of identity). *If a binary structure $(G, *)$ has an identity, then it is unique.*

It is now legitimate to refer to *the* identity e using the *definite article*. Uniqueness proofs in mathematics typically follow a pattern: suppose there are two such objects and show that they are identical.

Proof. Suppose $e, f \in G$ are identities. Then

$$ef = \begin{cases} f & \text{since } e \text{ is an identity} \\ e & \text{since } f \text{ is an identity} \end{cases}$$

We conclude that $f = e$. ∎

We used almost nothing about $(G, *)$; in particular it need not be associative (e.g. example 3).

Definition 2.6 (Inverse). Let $(G, *)$ have identity e. An element $x \in G$ has an *inverse* $y \in G$ if

$$xy = yx = e$$

Examples (ver. IV). 1. Every integer x has an inverse under addition: $x + (-x) = (-x) + x = 0$.

2. Since $(\mathbb{Z}, -)$ has no identity, the question of inverses makes no sense.
3. Since $e^2 = a^2 = ab = ba = e$, we see that every element has an inverse; indeed a has *two* inverses!

Element	e	a	b
Inverse(s)	e	a, b	a

Lemma 2.7 (Uniqueness of inverses). *Suppose $(G, *)$ is associative and has an identity. If $x \in G$ has an inverse, then it is unique.*

Proof. Suppose x has inverses $y, z \in G$. Then,

$$z(xy) = (zx)y \implies ze = ey \implies z = y$$

∎

Note where associativity was used in the proof. Example 3 shows that this condition is *necessary*: a non-associative structure can have non-unique inverses.

Definition 2.8 (Commutativity). Let $(G, *)$ be a binary structure. Elements $x, y \in G$ *commute* if $xy = yx$. We say that $*$ is *commutative* if all elements commute:

$$\forall x, y \in G,\ xy = yx$$

Examples (ver.V). 1. Addition of integers is commutative: $\forall x, y \in \mathbb{Z}$, $x + y = y + x$.

2. Subtraction is *non-commutative*: e.g. $2 - 3 \neq 3 - 2$.
3. The relation is commutative since its table is *symmetric* across its main $\searrow$ diagonal.

We simply assemble the pieces to obtain our main definition.

Definition 2.9 (Group axioms). A *group* is a binary structure $(G, *)$ satisfying the *associativity* and *identity* axioms, and for which all elements have *inverses*. This is summarized by the mnemonic

Closure, Associativity, Identity, Inverse

The *order* of G is its cardinality $|G|$. Moreover, G *abelian* if $*$ is *commutative.*

Of our examples, only $(\mathbb{Z}, +)$ is a group; indeed an *abelian*, *infinite* (order), *additive*[4] group (the operation is addition). The same observations show that $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are abelian groups.

Examples 2.10. 1. The non-zero real numbers $\mathbb{R}^\times$ forms an abelian group under multiplication.

Closure	If $x, y \neq 0$, then $xy \neq 0$
Associativity	$\forall x, y, z,\ x(yz) = (xy)z$
Identity	If $x \neq 0$, then $1 \cdot x = x \cdot 1 = x$, so $1 \in \mathbb{R}^\times$ is an identity
Inverse	Given $x \neq 0$, observe that $x^{-1} = \frac{1}{x}$ is an inverse: $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$
Commutativity	If $x, y \neq 0$, then $xy = yx$

Similarly, $(\mathbb{Q}^\times, \cdot)$ and $(\mathbb{C}^\times, \cdot)$ are abelian groups.

2. The *even* integers $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ form an abelian group under addition.
3. The *odd* integers $1 + 2\mathbb{Z} = \{1 + 2n : n \in \mathbb{Z}\}$ do not form a group under addition since they are not closed: for instance, $1 + 1 = 2 \notin 1 + 2\mathbb{Z}$.
4. Every vector space is an abelian group under addition.
5. $(\mathbb{R}, \cdot)$ is *not* a group, since 0 has no multiplicative inverse. Similarly $(\mathbb{Q}, \cdot)$, $(\mathbb{C}, \cdot)$ are not groups.
6. Groups of small order may be depicted in *Cayley tables*[5].

   Groups of orders 1, 2 and 3 are shown: you should check that these are groups.

   Note the *magic square property*: each row/column contains every element exactly once (see Exercise 13).

$*$	e
e	e

$*$	e	a
e	e	a
a	a	e

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

[4] The operation is addition; a *multiplicative* group follows the multiplication/juxtaposition convention. These are distinctions only of notation: e.g. $x + x + x = 3x$ in an additive group corresponds to $xxx = x^3$ in a multiplicative group.

[5] Englishman Arthur Cayley (1821–1895) was a pioneer of group theory. *Abelian* similarly honors the Norwegian mathematician Niels Abel (1802–1829).

Theorem 2.11 (Cancellation laws & inverses). *Suppose G is a group and $x, y, z \in G$. Then*

1. $xy = xz \implies y = z$
2. $xz = yz \implies x = y$
3. $(xy)^{-1} = y^{-1}x^{-1}$

Proof. The first two parts are exercises. For the third,

$$y^{-1}x^{-1}(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e$$

Thus $y^{-1}x^{-1}$ is an inverse of xy. Since inverses are unique, (Lemma 2.7) we are done. ∎

Associativity and Functional Composition

Theorem 2.12. *Let X be a set. Composition of functions $f : X \to X$ is associative.*

Proof. Let $f, g, h : X \to X$. We have equality $(f \circ g) \circ h = f \circ (g \circ h)$ if and only if these functions do the same thing to every element $x \in X$. But this is trivial:

$$\big((f \circ g) \circ h\big)(x) = (f \circ g)\big(h(x)\big) = f\big(g(h(x))\big) \quad \text{and,}$$
$$\big(f \circ (g \circ h)\big)(x) = f\big((g \circ h)(x)\big) = f\big(g(h(x))\big)$$

It follows that $\circ$ is associative. ∎

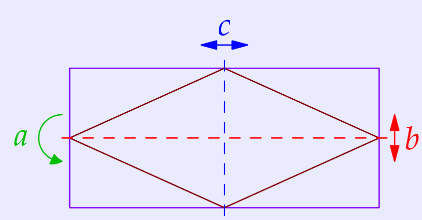
By viewing rotations and reflections as functions, the theorem verifies associativity for the following.

Corollary 2.13. *The* rotations *of a geometric figure form a group under composition.*
The symmetries (rotations and reflections) *of a geometric figure form a group under composition.*

Checking the other axioms is an exercise: the identity is considered a rotation (by 0°!).

Definition 2.14.
1. If ρ_k is rotation counter-clockwise by $\frac{2\pi k}{n}$ radians, then $R_n = \{\rho_0, \ldots, \rho_{n-1}\}$ is the *rotation group* of a regular n-gon.
2. The *dihedral group* D_n is the symmetry group of a regular n-gon.
3. The *Klein four-group*[6] (denoted V) is the symmetry group of a rectangle (or a rhombus), where a represents rotation by 180° and b, c are reflections.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



[6]From the German *Vierergruppe*. Felix Klein (1849–1925) was a pioneer in the application of group theory to geometry.

Since multiplication by an $n \times n$ matrix amounts to a function (e.g. $A \in M_n(\mathbb{R})$ corresponds to a linear map $\mathbb{R}^n \to \mathbb{R}^n : \mathbf{x} \mapsto A\mathbf{x}$), we immediately conclude:

Corollary 2.15. *Multiplication of square matrices is associative.*

Example 2.16. The *general linear group* comprises the invertible $n \times n$ matrices under multiplication

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$$

Invertibility is assumed, associativity is the corollary, and closure follows from the familiar result

$$\det AB = \det A \det B$$

Finally the identity is given by (drum roll...) the *identity matrix* $I = \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & \ddots & \\ & \ddots & \ddots & 0 \\ & & 0 & 1 \end{pmatrix}$!!
This group is *non-abelian* (when $n \geq 2$).

Look again at part 3 of Theorem 2.11: seem familiar?

Exercises 2.1. Key concepts/definitions: make sure you can state the formal definitions

Group (closure, associativity, identity, inverse) *Commutativity/abelian* *Cayley table* V $\mathrm{GL}_n(\mathbb{R})$

1. Given the binary operation table, calculate

   (a) $c * d$ (b) $a * (c * b)$

   (c) $(c * b) * a$ (d) $(d * c) * (b * a)$

$*$	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	a	d	c

2. A table for a binary operation on $\{a, b, c\}$ is given. Compute $a * (b * c)$ and $(a * b) * c$. Does the expression $a * b * c$ make sense? Explain why/why not.

$*$	a	b	c
a	b	c	b
b	c	a	a
c	b	a	c

3. Are the binary operations in the previous questions commutative? Explain.

4. (a) Describe (*don't write them all out!*) all possible binary operation tables on a set of two elements $\{a, b\}$. Of these, how many are commutative?

   (b) How many commutative/non-commutative operations are there on a set of n elements?

   (*Hint: a commutative table has what sort of symmetry?*)

5. Which are binary structures? For those that are, which are commutative and which associative?

   (a) $(\mathbb{Z}, *)$, $a * b = a - b$ (b) $(\mathbb{R}, *)$, $a * b = 2(a + b)$

   (c) $(\mathbb{R}, *)$, $a * b = 2a + b$ (d) $(\mathbb{R}, *)$, $a * b = \frac{a}{b}$

   (e) $(\mathbb{N}, *)$, $a * b = a^b$ (f) $(\mathbb{Q}^+, *)$, $a * b = a^b$, where $\mathbb{Q}^+ = \{x \in \mathbb{Q} : x > 0\}$

   (g) $(\mathbb{N}, *)$, $a * b =$ product of the distinct prime factors of ab. Also define $1 * 1 = 1$.

   (e.g. $42 * 10 = (2 \cdot 3 \cdot 7) * (2 \cdot 5) = 2 \cdot 3 \cdot 5 \cdot 7 = 210$)

6. For each axiom of an abelian group: if true, write it down; if false, provide a counter-example.
   (a) $\mathbb{N} = \{1, 2, 3, \ldots\}$ under addition.
   (b) $\mathbb{Q}$ under multiplication.
   (c) $X = \{a, b, c\}$ with $x * y := y$.
   (d) $\mathbb{R}^3$ with the cross/vector product $\times$.
   (e) For each $n \in \mathbb{R}$, the set $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ of multiples of n under addition.
7. Determine whether each of the following sets of matrices is a group under multiplication.
   (a) $\mathcal{K} = \{A \in \mathrm{M}_2(\mathbb{R}) : \det A = \pm 1\}$
   (b) $\mathcal{L} = \{A \in \mathrm{M}_2(\mathbb{R}) : \det A = 7\}$
   (c) $\mathcal{N} = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{R}) : ad \neq 0 \right\}$
8. (a) Prove the cancellation laws (Theorem 2.11 parts 1 & 2).
   (b) True or false: in a group, if $xy = e$, then $y = x^{-1}$.
   (c) In a (multiplicative) group, *prove* that $(x^{-1})^n = (x^n)^{-1}$ for any x and any $n \in \mathbb{N}$. How would we write this in an *additive* group (see footnote 4)?
9. Let G be a group. Prove the following:
   (a) $\forall x, y \in G,\ (xyx^{-1})^2 = xy^2x^{-1}$
   (b) $\forall x \in G,\ (x^{-1})^{-1} = x$
   (c) G is abelian $\iff \forall x, y \in G,\ (xy)^{-1} = x^{-1}y^{-1}$
10. (a) Suppose X contains at least two distinct elements $x \neq y$. Prove that there exist functions $f, g : X \to X$ for which $f \circ g \neq g \circ f$.
    (b) Show that multiplication of $n \times n$ matrices is non-commutative when $n \geq 2$.
11. (a) Describe the symmetry group and Cayley table of a non-equilateral isosceles triangle.
    (b) Explicitly state the Cayley table for the rotation group R_4 of a square.
    (c) Explain why the order of the dihedral group D_n is $2n$.
    (d) Prove the *rotation* part of Corollary 2.13.
12. Let $\mathcal{U}$ be a set and $\mathcal{P}(\mathcal{U})$ its power set (the set of subsets of $\mathcal{U}$).
    (a) Which of the group axioms is satisfied by the union operator $\cup$ on $\mathcal{P}(\mathcal{U})$?
    (b) Repeat part (a) for the intersection operator.
    (c) The *symmetric difference* of sets $A, B \subseteq \mathcal{U}$ is the set
    $$A \triangle B := (A \cup B) \setminus (A \cap B)$$
       i. Use Venn diagrams to give a sketch argument that $\triangle$ is associative on $\mathcal{P}(\mathcal{U})$.
       ii. Is $\big(\mathcal{P}(\mathcal{U}), \triangle\big)$ a group? Explain your answer.
13. (Magic Square) Suppose $(G, *)$ is associative and G is finite.
    Prove that $(G, *)$ is a group if and only if its (multiplication) table satisfies two conditions:
    i. One row and column (by convention the first) is a perfect copy of G itself.
    ii. Every element of G appears exactly once in each row and column.

2.2 Subgroups

In mathematics, the prefix *sub-* usually indicates a *subset* that retains whatever structure follows.

Definition 2.17 (Subgroup). Let G be a group. A *subgroup* of G is a subset $H \subseteq G$ which is a group with respect to the *same* binary operation; we write $H \leq G$.
A subgroup H is a *proper subgroup* if $H \neq G$; this is written $H < G$.
The *trivial subgroup* is the 1-element set $\{e\}$; all other subgroups are *non-trivial*.

Examples 2.18. The following are immediate from the definition:

1. $\{e\} \leq G$ and $G \leq G$ for *any* G
2. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$
3. $(\mathbb{Q}^\times, \cdot) < (\mathbb{R}^\times, \cdot) < (\mathbb{C}^\times, \cdot)$
4. $(\mathbb{R}^n, +) < (\mathbb{C}^n, +)$
5. $(2\mathbb{Z}, +) < (\mathbb{Z}, +)$
6. $(R_3, \circ) \leq (R_6, \circ)$ (rotation groups)

Thankfully you don't have to check all the group axioms to see that a subset is a subgroup.

Theorem 2.19 (Subgroup criterion). *Let G be a group. A non-empty subset $H \subseteq G$ is a subgroup if and only if it is closed under the group operation and inverses. Otherwise said,*

$$\forall h, k \in H,\ hk \in H \text{ and } h^{-1} \in H$$

Proof. $(\Rightarrow)$ H is a group and therefore satisfies all the axioms, including closure and inverse.
$(\Leftarrow)$ Since H is a subset of G, the group operation on G is automatically associative[7] on H. By assumption, H also satisfies the closure and inverse axioms, so it remains only to check the identity. Since $H \neq \emptyset$, we may choose some (any!) $h \in H$, from which

$$e = hh^{-1} \in H$$

since inverses and products remain in H. The identity e of G therefore in H, and so H is a group. ∎

Examples 2.20. 1. All the above examples can be confirmed using the theorem. For instance,

$$2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\} = \{2z : z \in \mathbb{Z}\}$$

is certainly a non-empty subset of the integers. Moreover, if $2m, 2n \in 2\mathbb{Z}$, then

$$2m + 2n = 2(m+n) \in 2\mathbb{Z} \quad \text{and} \quad -(2m) = 2(-m) \in 2\mathbb{Z}$$

whence $2\mathbb{Z}$ is closed under addition and inverses (negation).

2. The positive integers $\mathbb{N} = \{1, 2, \ldots\}$ are closed under addition but not inverses (for instance no $x \in \mathbb{N}$ satisfies $x + 2 = 0$). Thus $\mathbb{N}$ is not a subgroup of $\mathbb{Z}$ under addition.

3. Let $1 + 3\mathbb{Z}$ be the set of integers with remainder 1 when divided by 3:

$$1 + 3\mathbb{Z} = \{1 + 3n : n \in \mathbb{Z}\} = \{1, 4, 7, 10, 13, \ldots, -2, -5, -8, \ldots\}$$

Since $1 \in 1 + 3\mathbb{Z}$ but $1 + 1 = 2 \notin 1 + 3\mathbb{Z}$, we see that $1 + 3\mathbb{Z}$ is not a subgroup of $(\mathbb{Z}, +)$.

[7] Definition 2.3 makes no claim as to *where* $x(yz) = (xy)z$ lives!

Subgroup Diagrams It can be helpful to represent subgroup relations pictorially, where a descending line indicates a subgroup relationship. For instance, the diagram on the right summarizes *four* subgroup relations

$$\begin{tikzcd} & \mathbb{Z} \arrow[dl, dash] \arrow[dr, dash] & \\ 2\mathbb{Z} \arrow[dr, dash] & & 3\mathbb{Z} \arrow[dl, dash] \\ & 6\mathbb{Z} & \end{tikzcd}$$

$$6\mathbb{Z} < 2\mathbb{Z} < \mathbb{Z} \quad \text{and} \quad 6\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z}$$

where all four are groups under addition. If G has only *finitely many subgroups*, then its *subgroup diagram* is the complete depiction of all subgroups.

Matrix subgroups In Example 2.16 we saw that the invertible matrices $\mathrm{GL}_n(\mathbb{R})$ form a group under multiplication; here is one of its many subgroups, some others are in Exercise 10.

Example 2.21. The set $\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) : A^TA = I\}$ forms a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

- $I \in \mathrm{O}_n(\mathbb{R})$ so we have a non-empty set. Moreover, if $A \in \mathrm{O}_n(\mathbb{R})$, then

$$1 = \det I = \det A \det A^T = (\det A)^2 \implies \det A \neq 0 \implies A \in \mathrm{GL}_n(\mathbb{R})$$

- If $A, B \in \mathrm{O}_n(\mathbb{R})$, then

$$(AB)^T(AB) = B^TA^TAB = B^TIB = B^TB = I, \quad \text{and,}$$
$$(A^{-1})^TA^{-1} = (A^T)^TA^T = (AA^T)^T = I^T = I$$

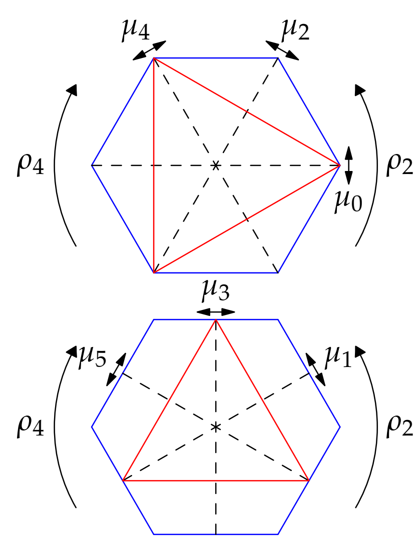
whence AB and $A^{-1} \in \mathrm{O}_n(\mathbb{R})$.

We call this the *orthogonal group*. When $n = 2$ or 3, its elements may be recognized as rotations and reflections. For instance, the matrix $\frac{1}{\sqrt{2}}\begin{pmatrix}1&-1\\1&1\end{pmatrix} \in \mathrm{O}_2(\mathbb{R})$ rotates $\mathbb{R}^2$ counter-clockwise by 45°.

Geometric subgroup proofs Arranging figures such that every symmetry of one is also a symmetry of the other immediately results in a subgroup relationship!

Example 2.22. A regular hexagon has symmetry group $D_6 = \{\rho_0, \ldots, \rho_5, \mu_0, \ldots, \mu_5\}$ consisting of six rotations and six reflections:

- ρ_k is rotation counter-clockwise by $60k°$; the identity is ρ_0.
- The μ_k are reflections across 'diameters' of the hexagon as indicated in the pictures below.



Now draw two equilateral triangles inside the hexagon. Each of the six symmetries of the equilateral triangle is also a symmetry of the hexagon! It follows that the symmetry group D_3 of the triangle is a subgroup of D_6 in two different ways:

$$\{e, \rho_2, \rho_4, \mu_0, \mu_2, \mu_4\} < D_6 \quad \text{and} \quad \{e, \rho_2, \rho_4, \mu_1, \mu_3, \mu_5\} < D_6$$

Exercises 2.2. Key concepts/definitions:

(Proper/trivial/non-trivial) Subgroup *Closure under operation/inverses* *Subgroup diagram*

1. Use Theorem 2.19 to verify that $\mathbb{Q}^\times$ is a subgroup of $\mathbb{R}^\times$ under multiplication.
2. Give two reasons why the *non-zero* integers do not form a subgroup of $\mathbb{Z}$ under addition.
3. Explain the relationship between positive integers m and n whenever $(m\mathbb{Z}, +) \leq (n\mathbb{Z}, +)$.
4. Prove or disprove: the set $H = \{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{N}_0\}$ forms a group under addition.
5. Use Theorem 2.19 to explain why the set of *rotations* of a planar geometric figure is a subgroup of the group of its rotations *and* reflections.
6. (a) Find the complete subgroup diagram of the Klein four-group.
   (b) Modelling Example 2.22, draw three pictures which describe different ways in which the Klein four-group may be viewed as a subgroup of D_6.
7. Find the subgroups and subgroup diagram of the rotation group $R_6 = \{\rho_0, \ldots, \rho_5\}$, where ρ_k is counter-clockwise rotation by $60k°$.
8. Suppose H and K are subgroups of G. Prove that $H \cap K$ is also a subgroup of G.
9. Let H be a non-empty subset of a group G. Prove that H is a subgroup of G if and only if

   $$\forall x, y \in H,\ xy^{-1} \in H$$

10. Prove that the following sets of matrices are groups under multiplication.
    (a) Special linear group: $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) : \det A = 1\}$
    (b) Special orthogonal group: $\mathrm{SO}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) : A^T A = I \text{ and } \det A = 1\}$
    (c) $\mathcal{Q}_n = \{A \in \mathrm{M}_n(\mathbb{R}) : \det A \in \mathbb{Q}^\times\}$
    (d) Symplectic group: $\mathrm{Sp}_{2n}(\mathbb{R}) = \{A \in \mathrm{M}_{2n}(\mathbb{R}) : A^T J A = J\}$, where $J = \left(\begin{array}{c|c} 0 & I_n \\ \hline -I_n & 0 \end{array}\right)$ is a block matrix and I_n the $n \times n$ identity matrix.
    (e) $\mathrm{SL}_n(\mathbb{Z}) = \{A \in \mathrm{M}_n(\mathbb{Z}) : \det A = 1\}$: all entries in these matrices are *integers.*
    (*Hint: look up the classical adjoint* adj A *of a square matrix*)

    Now construct a diagram showing the subgroup relationships between the groups

    $\mathrm{GL}_n(\mathbb{R}),\quad \mathrm{SL}_n(\mathbb{R}),\quad \mathrm{O}_n(\mathbb{R}),\quad \mathrm{SO}_n(\mathbb{R}),\quad \mathcal{Q}_n,\quad \mathrm{SL}_n(\mathbb{Z})$ (*ignore* $\mathrm{Sp}_{2n}(\mathbb{R})$)

11. The set $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ forms a group of order eight under 'multiplication' subject to the following properties:
    - 1 is the identity.
    - -1 commutes with everything; e.g. $(-1)i = -i = i(-1)$, etc.
    - $(-1)^2 = 1, \quad i^2 = j^2 = k^2 = -1$ and $ij = k$.
    - Multiplication is associative.

    (a) Find the Cayley table of $(Q_8, \cdot)$.
    (*Hint: You should easily be able to fill in 44 of 64 entries; now use associativity…*)
    (b) Find all subgroups of Q_8 and draw its subgroup diagram.

2.3 Homomorphisms & Isomorphisms

A key goal of abstract mathematics is the comparison of similar/identical structures with outwardly different appearances. We describe such comparisons using *functions.*

Definition 2.23 (Homomorphism). Suppose $(G, *)$ and $(H, \star)$ are binary structures and $\phi : G \to H$ a function. We say that ϕ is a *homomorphism* of binary structures if

$$\forall x, y \in G,\ \phi(x * y) = \phi(x) \star \phi(y)$$

For most of this course (certainly after this chapter), the binary structures will be groups.

Examples 2.24. 1. The function $\phi : (\mathbb{N}, +) \to (\mathbb{R}, +)$ defined by $\phi(x) = \sqrt{2}x$ is a homomorphism,

$$\phi(x + y) = \sqrt{2}(x + y) = \sqrt{2}x + \sqrt{2}y = \phi(x) + \phi(y)$$

It is worth spelling this out, since there are *two* ways to combine addition and ϕ:

- Sum $x + y$, then map to $\mathbb{R}$ to obtain $\phi(x + y)$.
- Map to $\mathbb{R}$, then sum to obtain $\phi(x) + \phi(y)$.

The homomorphism property says the results are *always identical.*

2. If V, W are vector spaces then every linear map $\mathrm{T} : V \to W$ is a group homomorphism:[8]

$$\forall \mathbf{v}_1, \mathbf{v}_2 \in V, \quad \mathrm{T}(\mathbf{v}_1 + \mathbf{v}_2) = \mathrm{T}(\mathbf{v}_1) + \mathrm{T}(\mathbf{v}_2)$$

This shows that you've been encountering homomorphisms your entire mathematical career, even in calculus: $\frac{\mathrm{d}}{\mathrm{d}x}(f + g) = \frac{\mathrm{d}f}{\mathrm{d}x} + \frac{\mathrm{d}g}{\mathrm{d}x}$ is a homomorphism property!

The most useful homomorphisms are *bijective*: these get a special name.

Definition 2.25 (Isomorphism). An *isomorphism* is a bijective/invertible homomorphism.[9]
We say that G and H are *isomorphic*, written $G \cong H$, if there exists an isomorphism $\phi : G \to H$.

Why do we care about isomorphisms? It is because isomorphic groups have exactly the same structure; one is simply a relabelled version of the other!
Here is the procedure for showing that binary structures $(G, *)$ and $(H, \star)$ are isomorphic:

Definition: Define $\phi : G \to H$ (if necessary). As we'll see starting in Chapter 3, if G is a set of equivalence classes you might need to check that ϕ is *well-defined.*

Homomorphism: Verify that $\phi(x * y) = \phi(x) \star \phi(y)$ for all $x, y \in G$.

Injectivity/1–1: Check $\phi(x) = \phi(y) \implies x = y$.

Surjectivity/onto: Check range $\phi = H$. Equivalently $\forall h \in H,\ \exists g \in G$ such that $h = \phi(g)$.

The last three steps can be done in any order. Injectivity/surjectivity might also be combined by exhibiting an explicit *inverse function* $\phi^{-1} : H \to G$.

[8] The scalar multiplication condition $\mathrm{T}(\lambda\mathbf{v}) = \lambda\mathrm{T}(\mathbf{v})$ of a linear map is not relevant here.
[9] These terms come from ancient Greek: *homo-* (similar, alike), *iso-* (equal, identical), and *morph(e)* (shape, structure).

Examples 2.26. 1. We show that $(2\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$ are isomorphic groups.

Definition: The obvious function is $\phi(x) = \frac{3}{2}x$; plainly $\phi(2m) = 3n$ whence $\phi : 2\mathbb{Z} \to 3\mathbb{Z}$.

Homomorphism: $\phi(x+y) = \frac{3}{2}(x+y) = \frac{3}{2}x + \frac{3}{2}y = \phi(x) + \phi(y)$

Injectivity: $\phi(x) = \phi(y) \implies \frac{3}{2}x = \frac{3}{2}y \implies x = y$.

Surjectivity: If $z = 3n \in 3\mathbb{Z}$, then $z = \frac{3}{2} \cdot \frac{2}{3}z = \frac{3}{2}(2n) = \phi(2n) \in \operatorname{range}\phi$.

In the last step we essentially observed that the inverse function is $\phi^{-1}(z) = \frac{2}{3}z$.

More generally, whenever $m, n \neq 0$, the groups $(m\mathbb{Z}, +)$ and $(n\mathbb{Z}, +)$ are isomorphic.

2. The function $\phi(x) = e^x$ is an isomorphism of abelian groups $\phi : (\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$.

   Definition: This is unnecessary since ϕ is given. However, note that both domain and codomain are *abelian groups* and that $\mathbb{R}^+ = (0, \infty)$ means the *positive real numbers.*

   Homomorphism: This is the familiar exponential law!

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$$

   Bijectivity: $\phi^{-1}(z) = \ln z$ is the inverse function of ϕ.

Non-isomorphicity & Structural Properties

Unless you have very small sets, you cannot realistically test every function $\phi : G \to H$ to see that structures are non-isomorphic! Instead we have to be a little more cunning.

Definition 2.27 (Structural properties). A *structural property* is any property which is preserved under isomorphism: i.e. if $\phi : (G, *) \to (H, \star)$ is an isomorphism then $(G, *)$ and $(H, \star)$ have identical structural properties.

The following is a non-exhaustive list of structural properties: we'll check a few in Exercise 6.

Cardinality/order: Since G and H are bijectively paired, their cardinalities are the same.

Commutativity & Associativity: For instance, if $*$ is commutative, then

$$\forall x, y \in G,\ \phi(x) \star \phi(y) = \phi(x * y) = \phi(y * x) = \phi(y) \star \phi(x)$$

Since ϕ is bijective, this says that $\star$ is commutative on H.

Identities & Inverses: For instance, if G has identity e, then $\phi(e)$ is the identity for H.

Solutions to equations: Related equations in G and H have the same number of solutions: e.g.

$$x * x = x \iff \phi(x) \star \phi(x) = \phi(x)$$

The equations $x * x = x$ and $z \star z = z$ therefore have the same number of solutions.

Being a group If G is a group, so also is H.

Examples 2.28.
1. The binary structures $(\mathbb{N}_0, +)$ and $(\mathbb{N}, +)$ are non-isomorphic, since $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ contains an identity element 0 while $\mathbb{N}$ does not.

2. The binary structures defined by the two tables are non-isomorphic; the first is commutative while the second is not.

$*$	a	b
a	a	b
b	b	a

$\star$	c	d
c	c	d
d	c	d

3. To see that $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are non-isomorphic groups, it is enough to recall that the sets have different cardinalities: $\mathbb{Q}$ is *countably infinite* while $\mathbb{R}$ is *uncountable.*

4. $\mathrm{GL}_2(\mathbb{R})$ and $(\mathbb{R}, +)$ have the same cardinality; however, since the first is non-abelian and the second abelian, the two groups are non-isomorphic.

Many properties are non-structural and therefore *cannot* be used to show non-isomorphicity: the type of element (number, matrix, etc.), the type of binary operation (addition, multiplication, etc.).

Transferring a Binary Structure

We can turn a bijection into an isomorphism by imposing the homomorphism property. If $(H, \star)$ and a bijection $\phi : G \to H$ are given, we can *define* a binary operation $*$ on G by *pulling-back* $\star$:

$$\forall x, y \in G,\ x * y := \phi^{-1}\big(\phi(x) \star \phi(y)\big)$$

Plainly $\phi : (G, *) \cong (H, \star)$ is an isomorphism! We can similarly *push-forward* a structure from G to H:

$$w \star z := \phi\big(\phi^{-1}(w) * \phi^{-1}(z)\big)$$

Example 2.29. $\phi(x) = x^3 + 8$ is a bijection $\mathbb{R} \to \mathbb{R}$. If $\phi : (\mathbb{R}, *) \to (\mathbb{R}, +)$ is an isomorphism, then

$$x * y := \phi^{-1}\big(\phi(x) + \phi(y)\big) = \phi^{-1}(x^3 + y^3 + 16) = \sqrt[3]{x^3 + y^3 + 8}$$

Since $(\mathbb{R}, +)$ is an abelian group and ϕ^{-1} an isomorphism, it follows that $(\mathbb{R}, *)$ is also an abelian group. Moreover, its identity must be

$$\phi^{-1}(0) = \sqrt[3]{-8} = -2$$

As a sanity check, observe that

$$x * (-2) = \sqrt[3]{x^3 + (-2)^3 + 8} = x$$

Up to Isomorphism: a common shorthand

This phrase is ubiquitous in abstract mathematics. For an example of how it is used, note that if $(\{e, a\}, *)$ is a group with identity e, then its Cayley table must be as shown (recall Example 2.10.6). This might be summarized by the phrase:

$*$	e	a
e	e	a
a	a	e

> *Up to isomorphism,* there is a unique group of order two.

More precisely: if G is *any* group of order two, then there exists an isomorphism $\phi : \{e, a\} \to G$. The expression 'up to isomorphism' is essential; without it, the sentence is *false*, since there are *infinitely many* distinct groups of order two!

Exercises 2.3. Key concepts/definitions:

Homomorphism *Injective/surjective/bijective* *Isomorphism* *Structural property* *'Up to isomorphism'*

1. Which of the following are homomorphisms/isomorphisms of binary structures? Explain.

   (a) $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +),\ \phi(n) = -n$

   (b) $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +),\ \phi(n) = n + 1$

   (c) $\phi : (\mathbb{Q}, +) \to (\mathbb{Q}, +),\ \phi(x) = \frac{4}{3}x$

   (d) $\phi : (\mathbb{Q}, \cdot) \to (\mathbb{Q}, \cdot),\ \phi(x) = x^2$

   (e) $\phi : (\mathbb{R}, \cdot) \to (\mathbb{R}, \cdot),\ \phi(x) = x^5$

   (f) $\phi : (\mathbb{R}, +) \to (\mathbb{R}, \cdot),\ \phi(x) = 2^x$

   (g) $\phi : (\mathrm{M}_2(\mathbb{R}), \cdot) \to (\mathbb{R}, \cdot),\ \phi(A) = \det A$

   (h) $\phi : (\mathrm{M}_n(\mathbb{R}), +) \to (\mathbb{R}, +)$, $\phi(A) = \operatorname{tr} A =$ trace of the matrix A (add the entries on the main diagonal).

2. Show that $(\mathbb{Z}, +) \cong (n\mathbb{Z}, +)$ for any *non-zero* constant n.

3. Prove or disprove: $(\mathbb{R}^3, +) \cong (\mathbb{R}^3, \times)$ (cross product).

4. $\phi(n) = 2 - n$ is a bijection of $\mathbb{Z}$ with itself. For each of the following, define a binary relation $*$ on $\mathbb{Z}$ such that ϕ is an isomorphism of binary relations.

   (a) $\phi : (\mathbb{Z}, *) \cong (\mathbb{Z}, +)$

   (b) $\phi : (\mathbb{Z}, *) \cong (\mathbb{Z}, \cdot)$

   (c) $\phi : (\mathbb{Z}, *) \cong (\mathbb{Z}, \max(a, b))$

5. $\phi(x) = x^2$ is a bijection $\phi : \mathbb{R}^+ \to \mathbb{R}^+$. Find $x * y$ if ϕ is to be an isomorphism of binary structures

   (a) $\phi : (\mathbb{R}^+, *) \to (\mathbb{R}^+, +)$

   (b) $\phi : (\mathbb{R}^+, +) \to (\mathbb{R}^+, *)$

6. Suppose $\phi : (G, *) \to (H, \star)$ is an isomorphism of binary structures. Prove the following:

   (a) If e is an identity for G, then $\phi(e)$ is an identity for H.

   (b) If $x \in G$ has an inverse y, then $\phi(x) \in H$ has an inverse $\phi(y)$.

   (c) If $*$ is associative, so is $\star$.

7. Let $\phi : (G, *) \to (H, \star)$ be a homomorphism of binary structures. Prove that the *image*

   $$\phi(G) = \operatorname{Im} \phi = \{\phi(x) : x \in G\}$$

   is closed under $\star$ (thus $(\phi(G), \star)$ is a binary structure). If $(G, *)$ and $(H, \star)$ are both groups, show that $\phi(G)$ is a subgroup of H.

8. Revisit Exercise 6a. Suppose e is an identity for $(G, *)$ and that $\phi : G \to H$ is merely a *homomorphism.* Must $\phi(e)$ be an identity for H? Explain why/why not: does it matter whether ϕ is a homomorphism of groups?

9. Let G be the group of rotations of the plane about the origin under composition.

   (a) Show that $\phi : (\mathbb{R}, +) \to G$ defined by

   $$\phi(x) = \text{rotate counter-clockwise } x \text{ radians}$$

   is a homomorphism of groups.

   (b) Prove or disprove: ϕ is an *isomorphism.*

10. (a) Prove that $S := \left\{ \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) \in M_2(\mathbb{R}) \right\}$ forms a group under matrix addition.

    (b) Prove that $T = S \setminus \{0\}$ (S except the zero matrix) forms a group under matrix *multiplication.*

    (c) Define $\phi \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) = a + ib$. Prove that $\phi : S \to \mathbb{C}$ and $\phi_T : T \to \mathbb{C}^\times$ are *both* isomorphisms

    $$\phi : (S, +) \cong (\mathbb{C}, +), \qquad \phi|_T : (T, \cdot) \cong (\mathbb{C}^\times, \cdot)$$

    (*In a future class, ϕ will be described as an isomorphism of rings/fields*)

11. The groups $(\mathbb{Q}, +)$ and $(\mathbb{Q}^+, \cdot)$ are both abelian and both have the same cardinality. Assume, for contradiction, that $\phi : \mathbb{Q} \to \mathbb{Q}^+$ is an isomorphism.

    (a) If $c \in \mathbb{Q}$ is constant, what equation in $\mathbb{Q}^+$ corresponds to $x + x = c$?

    (b) By considering how many solutions these equations have, obtain a contradiction and hence conclude that $(\mathbb{Q}, +) \not\cong (\mathbb{Q}^+, \cdot)$.

    (Extra challenge) Suppose $\psi : (\mathbb{Q}, +) \to (\mathbb{R}, \cdot)$ is a *homomorphism* and that $\psi(1) = a$: find a formula for $\psi(x)$.

12. Recall the magic square property (Exercise 2.1.13).

    (a) Up to isomorphism, explain why there is a unique group of order 3; its Cayley table should look like that of the rotation group R_3.

    (b) Show that there are only two ways to complete a Cayley table of order 4 up to isomorphism.
    (*Hints: if $G = \{e, a, b, c\}$, why may we assume, without loss of generality, that $b^2 = e$? Your answers should look like the Klein four-group V and the rotation group R_4.*)

13. Prove that *isomorphic* is an equivalence relation on any collection of groups: that is, for all groups G, H, K, we have

    Reflexivity $G \cong G$
    Symmetry $G \cong H \implies H \cong G$
    Transitivity $G \cong H$ and $H \cong K \implies G \cong K$

3 Cyclic groups

3.1 Definitions and Basic Examples

Cyclic groups are a basic family of groups whose complete structure can be easily described. The foundational idea is that a cyclic group can be generated by a single element.

Examples 3.1. 1. The group of integers $(\mathbb{Z}, +)$ is generated by 1. Otherwise said, all integers may be produced simply by combining 1 with itself using only the group operation $(+)$ and inverses $(-)$. Indeed, if n is a positive integer, then

$$n = 1 + 1 + \cdots + 1$$

The inverse operation produces $-n$, and the identity is $0 = 1 + (-1)$.

2. Recall the group $R_n = \{\rho_0, \ldots, \rho_{n-1}\}$ of rotations of a regular n-gon (Definition 2.14). Since $\rho_k = \rho_1^k$, the group is generated by ρ_1, the '1-step' counter-clockwise rotation by $\frac{2\pi}{n}$ radians.

We formalize this idea by considering a subset of a group G that is produced starting with a single element g. Since this is abstract, we follow the convention of writing G multiplicatively.

Lemma 3.2 (Cyclic subgroup). *Let G be a group and $g \in G$. The set*

$$\langle g \rangle := \{g^n : n \in \mathbb{Z}\} = \{\ldots, g^{-1}, e, g, g^2, \ldots\}$$

is a subgroup of G.

Proof. *Non-emptiness*: Plainly $e \in \langle g \rangle$.

Closure: Every element of $\langle g \rangle$ has the form g^k for some $k \in \mathbb{Z}$. The required condition is nothing more than standard exponential notation:

$$g^k \cdot g^l = g^{k+l} \in \langle g \rangle$$

Inverses: This is immediate by Exercise 2.1.8c: $(g^k)^{-1} = g^{-k} \in \langle g \rangle$. ∎

Definition 3.3 (Cyclic group). The subgroup $\langle g \rangle$ is the *cyclic subgroup of G generated by g*.
The *order* of an element $g \in G$ is the order (cardinality) $|\langle g \rangle|$ of the subgroup generated by g.
G is a *cyclic group* if $\exists g \in G$ such that $G = \langle g \rangle$: we call g a *generator* of G.

Warning! Don't confuse the *order of a group G* with the *order of an element $g \in G$*. Cyclic groups are the precisely those groups containing elements (generators) whose order equals that of the group.

Examples (3.1 cont). 1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ is generated by either 1 or -1. Note that this is an additive group, thus the subgroup generated by 2 is the group of even numbers under addition

$$\langle 2 \rangle = \{\ldots, -2, 0, 2, 4, \ldots\} = \{2m : m \in \mathbb{Z}\} = 2\mathbb{Z}$$

2. $R_n = \langle \rho_1 \rangle$. This group has other generators, but we'll delay finding them until the next section.

Modular Arithmetic

It is now time we introduced the most commonly encountered family of finite groups.

Definition 3.4. Let n be a positive integer. We denote by $\mathbb{Z}_n$ the set of *equivalence classes modulo n*.

It is most common to denote the elements of $\mathbb{Z}_n$ as *remainders*,[10] that is

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

You should be familiar with addition and multiplication modulo n, and you have several options for notation. For instance, here is a calculation in $\mathbb{Z}_5$ written four ways:

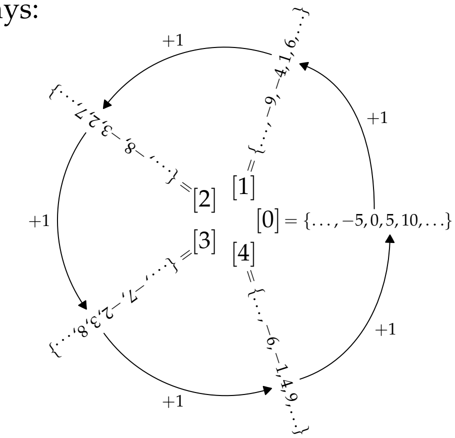
(a) Modular arithmetic: $4 + 2 \equiv 6 \equiv 1 \pmod 5$.

(b) Equivalence classes: $[4]_5 + [2]_5 = [6]_5 = [1]_5$.

(c) Decorate the operations: $4 +_5 2 = 6 = 1$.

(d) Drop almost all notation: $4 + 2 = 6 = 1$ in $\mathbb{Z}_5$.

Warning! If you choose version (d), you *must* make clear that you are working in $\mathbb{Z}_5$. If the distinction between numbers and equivalence classes is confusing, use one of the other notations!



Adding 1 in $\mathbb{Z}_5$

Theorem 3.5. *$\mathbb{Z}_n$ forms a cyclic, abelian group under addition modulo n.*

A direct rigorous proof is tedious right now. It will come for free in Chapter 6 when we properly define $\mathbb{Z}_n$ as a *factor group*. For the present, note simply that $\mathbb{Z}_n$ is cyclic since it is generated by 1.

Examples 3.6. Here are the Cayley tables for $\mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$.

$+_1$	0
0	0

$+_2$	0	1
0	0	1
1	1	0

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Compare these to Example 2.10.6.

[10] It is crucial to appreciate that these aren't numbers but *equivalence classes*. Thus $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ where the equivalence class $[x]$ of $x \in \mathbb{Z}$ is the set of integers with the same remainder as x:

$$[x] = \{z \in \mathbb{Z} : x \equiv z \pmod n\} = \{\ldots, x-n, x, x+n, x+2n \ldots\} = \{x + kn : k \in \mathbb{Z}\} = x + n\mathbb{Z}$$

Modular addition and multiplication of equivalence classes are *well-defined*. For addition: if $[x] = [w]$ and $[y] = [z]$, then $w = x + kn$ and $z = y + ln$ for some $k, l \in \mathbb{Z}$, from which

$$[w] +_n [z] = [w + z] = \big[(x + kn) + (y + ln)\big] = \big[x + y + n(k + l)\big] = [x + y] = [x] +_n [y]$$

All this should be familiar from a previous course. We'll revisit this in Chapter 6 when we define $\mathbb{Z}_n$ as a *factor group*.

These groups are typically the cyclic groups to which others are compared. Indeed, as we'll see shortly, any cyclic group of order n is isomorphic to $\mathbb{Z}_n$. For instance:

Example 3.7. $(\mathbb{Z}_3, +_3)$ is isomorphic to the rotation group $(R_3, \circ)$ via $\phi(k) = \rho_{k \pmod 3}$. It is worth doing this slowly, since the domain is a set of equivalence classes:

Well-definition: If $y = x \in \mathbb{Z}_3$, then $y \equiv x \equiv r \pmod 3$ for some $r \in \{0, 1, 2\}$. But then

$$\phi(y) = \rho_r = \phi(x)$$

Bijection: This is trivial $\phi : \{0, 1, 2\} \to \{\rho_0, \rho_1, \rho_2\}$.

Homomorphism: This is simply the formula for composition of rotations $\rho_k \rho_l = \rho_{k+l \pmod 3}$

The Roots of Unity

We finish with a third family of cyclic groups, viewed as subgroups of $(\mathbb{C}^\times, \cdot)$.

Aside: Notation Review $\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$ is the vector space $\mathbb{R}^2$ spanned by the basis $\{1, i\}$, where i is a 'number' satisfying $i^2 = -1$. Given $z = x + iy \in \mathbb{C}$, we consider several objects:

Complex conjugate: $\overline{z} = x - iy$ is the reflection of z in the real axis

Modulus (length): $r = |z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2}$

Argument (angle): $\theta = \arg z$ is the angle measured counter-clockwise from the positive real axis to $\overrightarrow{0z}$ (if $z \neq 0$).

Polar form: $z = re^{i\theta} = r\cos\theta + ir\sin\theta$

The modulus and argument are the usual polar co-ordinates. When $r = 1$ we have *Euler's formula*:[11]

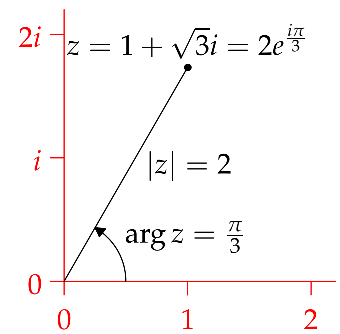
$$e^{i\theta} = \cos\theta + i\sin\theta$$

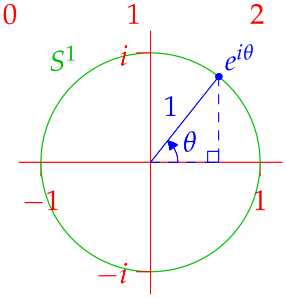
the source of the famous identity $e^{i\pi} = -1$. In the picture, S^1 denotes the unit circle. Note also that

$$e^{i\theta} = 1 \iff \theta = 2\pi k \quad \text{for some integer } k \qquad (\dagger)$$

The polar form behaves nicely with respect to multiplication:

$$|zw| = |z|\,|w| \quad \text{and} \quad \arg(zw) \equiv \arg z + \arg w \pmod{2\pi}$$





Definition 3.8. Let $n \in \mathbb{N}$. The n^{th} *roots of unity*[12] comprise the cyclic subgroup of $\mathbb{C}^\times$ generated by $\zeta := e^{\frac{2\pi i}{n}}$:

$$U_n := \langle \zeta \rangle = \{1, \zeta, \zeta^2, \cdots, \zeta^{n-1}\}$$

[11] More generally, if $x, y \in \mathbb{R}$, then $e^{x+iy} = e^x e^{iy} = e^x \cos y + ie^x \sin y$.

[12] In this context, *unity* is just a pretentious term for the number one!

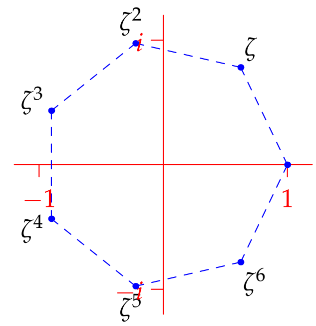
If necessary, write $\zeta_n = e^{\frac{2\pi i}{n}}$ to emphasize n.

The square roots of unity are simply ± 1, and we saw the 4^{th} roots $\pm 1, \pm i$ in Example 3.1. The n^{th} roots are equally spaced round the unit circle at the vertices of a regular n-gon; this is since

$$\arg \zeta^k = \arg e^{\frac{2\pi k}{n}} = \frac{2\pi k}{n} = k \arg \zeta$$

We stop listing the elements of U_n at ζ^{n-1}, since $\zeta^n = e^{2\pi i} = 1$. Indeed, by (†), we see the relationship with modular arithmetic

$$\zeta^k = \zeta^l \iff 1 = \zeta^{k-l} = e^{\frac{2\pi i(k-l)}{n}} \iff k \equiv l \pmod{n}$$



Seventh roots: $\zeta_7 = e^{\frac{2\pi i}{7}}$

Theorem 3.9. *The n^{th} roots of unity are precisely the n (complex) roots of the equation $z^n = 1$.*

Proof. Plainly $(\zeta^k)^n = (e^{\frac{2\pi ik}{n}})^n = e^{2\pi ik} = 1$, so every element of U_n solves $z^n = 1$.
For the converse, suppose $z^n = 1$. Take the modulus to obtain $|z|^n = 1$. Since $|z|$ is a non-negative real number, we see that $|z| = 1$, whence its polar form is $z = e^{i\theta}$. Now compute:

$$1 = z^n = (e^{i\theta})^n = e^{in\theta} \iff n\theta = 2\pi k$$

for some integer k (∗). But then $\theta = \frac{2\pi k}{n}$ and so

$$z = e^{i\theta} = e^{\frac{2\pi i}{n}k} = \left(e^{\frac{2\pi i}{n}}\right)^k = \zeta^k$$

■

In fact U_n is just the rotation group $R_n = \{\rho_0, \ldots, \rho_{n-1}\}$ in disguise!

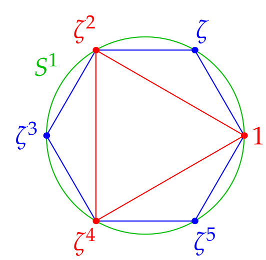
Lemma 3.10. *For any $z \in \mathbb{C}$, $\zeta_n^k z = \rho_k(z)$ is the result of rotating z counter-clockwise by $\frac{2\pi k}{n}$ radians.*

Examples 3.11. 1. Observe that $\zeta_6^2 = (e^{\frac{2\pi i}{6}})^2 = e^{\frac{2\pi i}{3}} = \zeta_3$.

We immediately obtain a subgroup relationship: with $\zeta = \zeta_6$,

$$U_3 = \{1, \zeta^2, \zeta^4\} < U_6 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$$

This is essentially trivial by drawing a picture!



2. The group table for U_n is trivial to construct. Here is U_3, where we use the fact that $\zeta^3 = 1$: if we write the table with $1 = \zeta^0$ and $\zeta = \zeta^1$, the relationship to $(\mathbb{Z}_3, +_3)$ and $(R_3, \circ)$ is glaring:

$\cdot$	1	ζ	ζ^2
1	1	ζ	ζ^2
ζ	ζ	ζ^2	1
ζ^2	ζ^2	1	ζ

$\cdot$	ζ^0	ζ^1	ζ^2
ζ^0	ζ^0	ζ^1	ζ^2
ζ^1	ζ^1	ζ^2	ζ^0
ζ^2	ζ^2	ζ^0	ζ^1

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\circ$	ρ_0	ρ_1	ρ_2
ρ_0	ρ_0	ρ_1	ρ_2
ρ_1	ρ_1	ρ_2	ρ_0
ρ_2	ρ_2	ρ_0	ρ_1

More formally, the groups are *isomorphic* $(U_3, \cdot) \cong (\mathbb{Z}_3, +_3) \cong (R_3, \circ)$.

Exercises 3.1. Key concepts/definitions:

Generator *Order of an element* *Cyclic (sub)group* $\mathbb{Z}_n$ *Roots of unity*

1. State the Cayley tables for $(\mathbb{Z}_5, +_5)$ and $(\mathbb{Z}_6, +_6)$.
2. List *all* the generators of each cyclic group.
   (a) $(\mathbb{Z}, +)$.
   (b) $\{2^n 3^{-n} : n \in \mathbb{Z}\}$ under multiplication.
   (c) $\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix} : a, b = \pm 1 \right\}$ under multiplication.
3. Revisit Example 1.2. What is the cyclic subgroup of D_3 generated by ρ_1? Generated by μ_1?
4. Explicitly compute the cyclic subgroup $\langle \zeta_8^5 \rangle$ of U_8, listing its elements in the order generated.
5. The *circle group* is the set $S^1 = \{e^{i\theta} : \theta \in [0, 2\pi)\}$. Prove that S^1 is a subgroup of $\mathbb{C}^\times$ under multiplication.
6. (a) Prove that $(U_3, \cdot)$ is a subgroup of $(U_9, \cdot)$.
   (b) Complete the sentence and prove your assertion:
   $U_m \leq U_n$ if and only if ____(relationship between m and n)____
7. (a) Show that the set $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$ forms a cyclic group under *multiplication* modulo 5.
   (b) What about the set $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ under multiplication modulo 8? To what previously encountered group is this isomorphic?
8. (a) Explain why $\{1, 2, 3, 4, 5\}$ isn't a group under multiplication modulo 6.
   (b) Hypothesize for which integers $n \geq 2$ the set $\{1, 2, 3, \ldots, n-1\}$ is a group under multiplication modulo n. If you want a challenge, try to prove your assertion.
9. Verify that $\phi : \mathbb{C} \to \mathbb{C}^\times : z \mapsto e^z$ is a homomorphism of abelian groups $(\mathbb{C}, +), (\mathbb{C}^\times, \cdot)$ but *not* an isomorphism.
   (*This is in contrast to the real case: Example 2.26.2*)
10. (a) Prove Lemma 3.10.
    (b) Use the Lemma to prove that $(U_n, \cdot)$ and $(R_n, \circ)$ are isomorphic groups.

3.2 The Classification and Structure of Cyclic Groups

In this abstract section, we describe all cyclic groups, their generators, and subgroup structures.

Lemma 3.12. *Every cyclic group is abelian.*

Proof. Let $G = \langle g \rangle$. Since any two elements of G can be written g^k, g^l for some $k, l \in \mathbb{Z}$, we immediately see that

$$g^k g^l = g^{k+l} = g^{l+k} = g^l g^k$$

∎

Note that the converse is false: the Klein four-group V is abelian but not cyclic.

Theorem 3.13 (Isomorphs). *Every cyclic group is isomorphic either to $(\mathbb{Z}, +)$ or to some $(\mathbb{Z}_n, +_n)$. In either case, if $G = \langle g \rangle$, then $\phi : x \mapsto g^x$ defines an isomorphism $\mathbb{Z}_{(n)} \cong G$.*

Proof. To distinguish these cases, consider the set of natural numbers

$$S = \{m \in \mathbb{N} : g^m = e\}$$

If $S = \emptyset$: Suppose $x > y$ and that $g^x = g^y$. Then $g^{x-y} = e \implies x - y \in S$: contradiction. It follows that the elements $\ldots, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots$ are distinct and that $\phi : \mathbb{Z} \to G$ is a bijection.

If $S \neq \emptyset$: Let[13] $n = \min S$ and define $\phi : \mathbb{Z}_n \to G : x \mapsto g^x$. We check that this is well-defined:

$$\begin{aligned} y = x \in \mathbb{Z}_n &\implies y = x + kn \text{ for some } k \in \mathbb{Z} \\ &\implies \phi(y) = g^y = g^{x+kn} = g^x (g^n)^k = g^x = \phi(x) \end{aligned}$$

Since the highlighted calculation is valid for all $x, k \in \mathbb{Z}$, we also conclude that

$$G = \langle g \rangle \subseteq \{e, g, \ldots, g^{n-1}\}$$

contains *finitely many* terms. Suppose two of these were equal; if $0 \leq y \leq x \leq n-1$, then

$$g^x = g^y \implies g^{x-y} = e \implies x = y$$

since $0 \leq x - y < n - 1$ and $n = \min S$. Thus n is the order of G and $G = \{e, g, \ldots, g^{n-1}\}$.

In both cases, the homomorphism property is simply the exponential law

$$\phi(x + y) = g^{x+y} = g^x g^y = \phi(x)\phi(y)$$

∎

The set S quickly yields an alternative measure for the order of an element.

Corollary 3.14. *If $G = \langle g \rangle$ is finite, then its order is the smallest positive integer n such that $g^n = e$. Moreover $g^m = e \iff m$ is a multiple of n ($n \mid m$).*

[13] By the well-ordering property of the natural numbers, any non-empty subset has a minimum element.

Examples 3.15. 1. The group of 7^{th} roots of unity $(U_7, \cdot)$ is isomorphic to $(\mathbb{Z}_7, +_7)$ via

$$\phi : \mathbb{Z}_7 \to U_7 : k \mapsto \zeta_7^k$$

2. The additive group $5\mathbb{Z} = \{5z : z \in \mathbb{Z}\}$ is infinite and cyclic. It is isomorphic to the integers via

$$\phi : (\mathbb{Z}, +) \cong (5\mathbb{Z}, +) : z \mapsto 5z$$

3. Let $\zeta = e^{\frac{2\pi i}{\sqrt{2}}}$ and consider the cyclic subgroup $G := \langle \zeta \rangle < (\mathbb{C}^\times, \cdot)$. For integers m, observe that

$$\zeta^m = e^{\frac{2\pi i m}{\sqrt{2}}} = 1 \iff \frac{m}{\sqrt{2}} \in \mathbb{Z} \iff m = 0$$

We conclude that G is an infinite cyclic group and that $\phi : \mathbb{Z} \to G : z \mapsto \zeta^z$ is an isomorphism. We can interpret ζ as performing an irrational fraction $(\frac{1}{\sqrt{2}})$ of a full rotation.

4. $(\mathbb{R}, +)$ is non-cyclic since its (uncountable) cardinality $2^{\aleph_0}$ is larger than the (countable) cardinality $\aleph_0$ of the integers. This is also straightforward to see directly: if $\mathbb{R}$ were cyclic with generator x, then we'd obtain an immediate contradiction

$$\frac{x}{2} \notin \{\ldots, -2x, -x, 0, x, 2x, 3x \ldots\} = \mathbb{R} \ni \frac{x}{2}$$

The same argument shows that $(\mathbb{Q}, +)$ is not cyclic.

Subgroups of Cyclic Groups

We can straightforwardly classify all subgroups of a cyclic group: they're also cyclic!

Theorem 3.16. *Any subgroup of a cyclic group is cyclic.*

The motivation for the proof is simple: the subgroup $2\mathbb{Z} \leq \mathbb{Z}$ is generated by 2, the minimal *positive* integer in the subgroup. Given a general subgroup $H \leq G$, we identify a suitable 'minimal' element, then demonstrate that this generates our subgroup.

Proof. Suppose $H \leq G = \langle g \rangle$. If $H = \{e\}$ is trivial, we are done: H is cyclic!
Otherwise, $\exists s \in \mathbb{N}$ minimal such that $g^s \in H$. We claim that $H = \langle g^s \rangle$: i.e. H is generated by g^s.

$(\langle g^s \rangle \subseteq H)$ This is trivial since $g^s \in H$.

$(H \subseteq \langle g^s \rangle)$ Let $g^m \in H$. By the division algorithm, there exist unique integers q, r such that

$$m = qs + r \quad \text{and} \quad 0 \leq r < s$$

But then

$$g^m = g^{qs+r} = (g^s)^q g^r \implies g^r = (g^s)^{-q} g^m \in H$$

since H is closed under $\cdot$ and inverses. By the minimality of S, this forces $r = 0$, from which we conclude that $g^m = (g^s)^q \in \langle g^s \rangle$.

∎

The infinite case is particularly simple; the proof is an exercise.

Corollary 3.17 (Subgroups of infinite cyclic groups). *If G is an infinite cyclic group and $H \leq G$, then either $H = \{e\}$ is trivial, or $H \cong G$.*

Example 3.18. It is helpful to write this out explicitly in additive notation when $G = \mathbb{Z}$. Since every subgroup is cyclic, there are two cases:

- The trivial subgroup: $\langle 0 \rangle = \{0\}$.
- Every other subgroup: $\langle s \rangle = s\mathbb{Z}$ when $s \neq 0$. All of these subgroups are isomorphic to $\mathbb{Z}$ via the isomorphism $\phi : \mathbb{Z} \to s\mathbb{Z} : x \mapsto sx$.

Finite cyclic groups are a little more complicated, so it is worth seeing an example first.

Example 3.19. Consider $U_6 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ under multiplication. Since all subgroups are cyclic, we need only consider what is generated by each element.

x	subgroup $\langle x \rangle$
1	$\{1\}$
ζ	$\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$
ζ^2	$\{1, \zeta^2, \zeta^4\}$
ζ^3	$\{1, \zeta^3\}$
ζ^4	$\{1, \zeta^4, \zeta^2\}$
ζ^5	$\{1, \zeta^5, \zeta^4, \zeta^3, \zeta^2, \zeta\}$

$$\begin{tikzcd} & \langle \zeta \rangle = U_6 \arrow[dl, dash] \arrow[dr, dash] & \\ \langle \zeta^2 \rangle = U_3 \arrow[dr, dash] & & \langle \zeta^3 \rangle = U_2 \arrow[dl, dash] \\ & \langle 1 \rangle = U_1 & \end{tikzcd}$$

Observe the repetitions: $\langle \zeta \rangle = \langle \zeta^5 \rangle = U_6$ and $\langle \zeta^2 \rangle = \langle \zeta^4 \rangle = U_3$.

For comparison, here is the same data for subgroups of the additive group $(\mathbb{Z}_6, +_6)$.

x	subgroup $\langle x \rangle$
0	$\{0\}$
1	$\{0, 1, 2, 3, 4, 5\}$
2	$\{0, 2, 4\}$
3	$\{0, 3\}$
4	$\{0, 4, 2\}$
5	$\{0, 5, 4, 3, 2, 1\}$

$$\begin{tikzcd} & \langle 1 \rangle = \mathbb{Z}_6 \arrow[dl, dash] \arrow[dr, dash] & \\ \langle 2 \rangle \cong \mathbb{Z}_3 \arrow[dr, dash] & & \langle 3 \rangle \cong \mathbb{Z}_2 \arrow[dl, dash] \\ & \langle 0 \rangle \cong \mathbb{Z}_1 & \end{tikzcd}$$

The difference is almost entirely notational, as must be since the groups are isomorphic. Note, however, in the subgroup diagram that we can't use *equals* as we did for U_6: for instance, $\langle 2 \rangle = \{0, 2, 4\}$ is *isomorphic* but *not equal* to $\mathbb{Z}_3 = \{0, 1, 2\}$.

You should be able to guess two patterns from the example:

- $\mathbb{Z}_n$ has exactly one subgroup of order d for each divisor d of n.
- If $d \in \mathbb{Z}_n$ is a divisor of n, then $\langle d \rangle \cong \mathbb{Z}_{\frac{n}{d}}$.

Corollary 3.20 (Subgroups of finite cyclic groups). *Let $G = \langle g \rangle$ have order n. Then G has a unique subgroup of each order dividing n. More precisely,*

$$d = \gcd(s, n) \implies \langle g^s \rangle = \langle g^d \rangle \cong \mathbb{Z}_{\frac{n}{d}}$$

Proof. Suppose $d = \gcd(s, n)$. We show first that $\langle g^s \rangle = \langle g^d \rangle$.

$(\langle g^s \rangle \subseteq \langle g^d \rangle)$ Since $d \mid s$ we have $s = kd$ for some $k \in \mathbb{Z}$, and so

$$(g^s)^m = (g^d)^{mk} \in \langle g^d \rangle \implies \langle g^s \rangle \subseteq \langle g^d \rangle$$

$(\langle g^s \rangle \supseteq \langle g^d \rangle)$ By Bézout's identity (ext. Euclidean alg.), $d = \kappa s + \lambda n$ for some $\kappa, \lambda \in \mathbb{Z}$, whence

$$g^d = (g^s)^\kappa (g^n)^\lambda = (g^s)^\kappa \in \langle g^s \rangle \implies \langle g^d \rangle \subseteq \langle g^s \rangle$$

To finish, we *count* the number of elements in $\langle g^d \rangle$. Since $d \mid n$, there are precisely $\frac{n}{d}$ of these, namely

$$\langle g^d \rangle = \{e, g^d, g^{2d}, \ldots, g^{n-d}\}$$

■

The result is worth restating explicitly in the additive group $(\mathbb{Z}_n, +_n)$:

$$d = \gcd(s, n) \implies \langle s \rangle = \langle d \rangle \cong \mathbb{Z}_{\frac{n}{d}}$$

In particular: $x \in \mathbb{Z}_n$ is a generator if and only if $\gcd(x, n) = 1$.

Example 3.21. We describe all subgroups of $\mathbb{Z}_{30}$ and construct its subgroup diagram. The first column lists the subgroup generated by each value $x \in \mathbb{Z}_{30}$. The second column is the isomorphic group $\mathbb{Z}_{\frac{30}{d}}$. The final column lists the divisors d of 30, and thus the possible values of $\gcd(x, 30)$.

Subgroup $\langle x \rangle$	Isomorph $\mathbb{Z}_{\frac{30}{d}}$	$d = \gcd(x, 30)$
$\{\ldots, 1, \ldots, 7, \ldots, 11, \ldots, 13, \ldots, 17, \ldots, 19, \ldots, 23, \ldots, 29\}$	$\mathbb{Z}_{30}$	1
$\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\}$	$\mathbb{Z}_{15}$	2
$\{0, 3, 6, 9, 12, 15, 18, 21, 24, 27\}$	$\mathbb{Z}_{10}$	3
$\{0, 5, 10, 15, 20, 25\}$	$\mathbb{Z}_6$	5
$\{0, 6, 12, 18, 24\}$	$\mathbb{Z}_5$	6
$\{0, 10, 20\}$	$\mathbb{Z}_3$	10
$\{0, 15\}$	$\mathbb{Z}_2$	15
$\{0\}$	$\mathbb{Z}_1$	0 (30)

The subgroup diagram is drawn, with the obvious (minimal) generator chosen for each subgroup; any of the other generators in the table could have been chosen instead.

With a little thinking, you should appreciate that the *shape* of the subgroup diagram (this one looks a little like a cube…) depends only on the *prime factorization* $30 = 2 \cdot 3 \cdot 5$; namely that each prime appears exactly once in the decomposition.

$$\begin{tikzcd}
 & \langle 1 \rangle = \mathbb{Z}_{30} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle 2 \rangle \cong \mathbb{Z}_{15} \arrow[d, dash] \arrow[dr, dash] & \langle 3 \rangle \cong \mathbb{Z}_{10} \arrow[dl, dash] \arrow[dr, dash] & \langle 5 \rangle \cong \mathbb{Z}_6 \arrow[dl, dash] \arrow[d, dash] \\
\langle 6 \rangle \cong \mathbb{Z}_5 \arrow[dr, dash] & \langle 10 \rangle \cong \mathbb{Z}_3 \arrow[d, dash] & \langle 15 \rangle \cong \mathbb{Z}_2 \arrow[dl, dash] \\
 & \langle 0 \rangle \cong \mathbb{Z}_1 &
\end{tikzcd}$$

Exercises 3.2. Key concepts:

Every cyclic group isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$ $\quad$ *$\langle g\rangle$ order $n \implies \langle g^s\rangle$ order $\frac{n}{\gcd(s,n)}$*

Subgroup diagrams for finite cyclic groups

1. For each group: construct the subgroup diagram and give a generator of each subgroup.

   (a) $(\mathbb{Z}_{10}, +_{10})$ $\qquad$ (b) $(\mathbb{Z}_{42}, +_{42})$.

2. A generator of the cyclic group U_n group is known as a *primitive n^{th} root of unity.* For instance, the primitive 4^{th} roots are $\pm i$. Find all the primitive roots when:

   (a) $n = 5$ $\qquad$ (b) $n = 6$ $\qquad$ (c) $n = 8$ $\qquad$ (d) $n = 15$

3. Find the complete subgroup diagram of U_{p^2q} where p, q are distinct primes.

   (*Hint: try U_{12} first if this seems too difficult*)

4. If $r \in \mathbb{N}$ and p is prime, find all subgroups of $(\mathbb{Z}_{p^r}, +_{p^r})$ and give a generator for each.

5. (a) Suppose $\phi : G \to H$ is an isomorphism of cyclic groups. If g is a generator of G, prove that $\phi(g)$ is a generator of H. Do you really need ϕ to be an *isomorphism* here?

   (b) If G is an infinite cyclic group, how many generators has it?

   (c) Recall Exercise 3.1.7a. Describe an isomorphism $\phi : \mathbb{Z}_4 \to \mathbb{Z}_5^\times$.

6. True or false: In *any* group G, if g has order n, then g^s has order $\frac{n}{\gcd(s,n)}$. Explain your answer.

7. Suppose $G = \langle g\rangle$ is infinite and $H = \langle g^s\rangle$ is an infinite subgroup. Prove Corollary 3.17 by explicitly finding an isomorphism $\phi : G \to H$.

8. Prove Corollary 3.14: you'll need the division algorithm for the second part!

9. Let x, y be elements of a group G. If xy has finite order n, prove that yx also has order n.

   (*Hint:* $(xy)^m = x(yx)^{m-1}y$)

10. Let $\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$ be the set of generators of the additive group $(\mathbb{Z}_n, +_n)$. Prove that $\mathbb{Z}_n^\times$ is a group under *multiplication* modulo n.

    (*Hint: You need Bézout's identity. This is the group of units in the ring* $(\mathbb{Z}_n, +_n, \cdot_n)$)

11. Let G be a group and X a non-empty subset of G. The *subgroup generated by X* is the subgroup created by making all possible combinations of elements and inverses of elements in X.

    (a) Explain why $(\mathbb{Z}, +)$ is generated by the set $X = \{2, 3\}$.

    (b) If $m, n \in (\mathbb{Z}, +)$, show that the group generated by $X = \{m, n\}$ is $d\mathbb{Z}$, where $d = \gcd(m, n)$.

    (c) The Klein four-group V is not-cyclic, so it cannot be generated by a singleton set. Find a set of *two* elements which generates V.

    (d) Describe the subgroup of $(\mathbb{Q}, +)$ generated by $X = \{\frac{1}{2}, \frac{1}{3}\}$.

    (e) (Hard) $(\mathbb{Q}, +)$ is plainly generated by the *infinite* set $\{\frac{1}{n} : n \in \mathbb{N}\}$. Explain why $(\mathbb{Q}, +)$ is *not finitely generated*: i.e. there exists no *finite* set X generating $\mathbb{Q}$.

    (*Hint: think about the prime factors of the denominators of elements of X*)

4 Direct Products & Finitely Generated Abelian Groups

In this short chapter we see a straightforward way to create new groups from old using the *Cartesian product.*

Example 4.1. Given $\mathbb{Z}_2 = \{0,1\}$, the Cartesian product

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \big\{(0,0),(0,1),(1,0),(1,1)\big\}$$

has four elements. This set inherits a *group structure* in a natural way by adding co-ordinates

$$(x,y)+(v,w) := (x+v, y+w)$$

where $x+v$ and $y+w$ are computed in $(\mathbb{Z}_2,+_2)$. This is a binary operation on $\mathbb{Z}_2 \times \mathbb{Z}_2$, with a familiar-looking table: it has exactly the same structure as the Cayley table for the Klein four-group!

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

$\leftrightsquigarrow$

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

We conclude that $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$ is indeed a group.

This construction works in general.

Theorem 4.2 (Direct product). *The natural component-wise operation on the Cartesian product*

$$\prod_{k=1}^{n} G_k = G_1 \times \cdots \times G_n, \qquad (x_1,\ldots,x_n)\cdot(y_1,\ldots,y_n) := (x_1y_1,\ldots,x_ny_n)$$

defines a group structure: the direct product. *This is abelian if each G_k is abelian.*

The proof is a simple exercise. Being a Cartesian product, a direct product has order equal to the product of the orders of its components

$$\left|\prod_{k=1}^{n} G_k\right| = \prod_{k=1}^{n} |G_k|$$

Examples 4.3. 1. Consider the direct product of groups $(\mathbb{Z}_2,+_2)$ and $(\mathbb{Z}_3,+_3)$:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \big\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\big\}$$

This is abelian and has order 6, so we might guess that it is isomorphic to $(\mathbb{Z}_6,+_6)$. To see this we need a generator: choose $(1,1)$ and observe that

$$\langle(1,1)\rangle = \big\{(1,1),(0,2),(1,0),(0,1),(1,2),(0,0)\big\} = \mathbb{Z}_2 \times \mathbb{Z}_3$$

The map $\phi(x) = (x,x)$ is therefore an isomorphism $\phi : \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

2. If each G_k is *abelian, written additively*, the direct product can instead be called the *direct sum*

$$\bigoplus_{k=1}^{n} G_k = G_1 \oplus \cdots \oplus G_n$$

We won't use this notation,[14] though you've likely encountered it in linear algebra: the direct sum of n copies of the real line $\mathbb{R}$ is the familiar vector space

$$\mathbb{R}^n = \bigoplus_{i=1}^{n} \mathbb{R} = \mathbb{R} \oplus \cdots \oplus \mathbb{R}$$

Orders of Elements in a Direct Product

In Example 4.3.1, we saw that the element $(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ had order 6 and thus generated the group. To help spot the pattern, consider another example.

Example 4.4. What is the order of the element $(10,2) \in \mathbb{Z}_{12} \times \mathbb{Z}_8$? Recall Corollary 3.20:

- $10 \in \mathbb{Z}_{12}$ has order $6 = \frac{12}{\gcd(10,12)}$
- $2 \in \mathbb{Z}_8$ has order $4 = \frac{8}{\gcd(2,8)}$

If we repeatedly add $(10,2)$, then the first co-ordinate will reset after 6 summations, while the second resets after 4. For *both* to reset, we need a *common multiple* of 6 and 4 summands. We can check this explicitly:

$$\langle(10,2)\rangle = \{(10,2),(8,4),(6,6),(4,0),(2,2),(0,4),(10,6),(8,0),(6,2),(4,4),(2,6),(0,0)\}$$

The order of the element $(10,2)$ is indeed the *least common multiple* $12 = \operatorname{lcm}(6,4)$.

Theorem 4.5. *Suppose $x_k \in G_k$ has order r_k. Then $(x_1,\ldots,x_n) \in \prod_{k=1}^{n} G_k$ has order $\operatorname{lcm}(r_1,\ldots,r_n)$.*

Proof. Just appeal to Corollary 3.14:

$$(x_1,\ldots,x_n)^m = (x_1^m,\ldots,x_n^m) = (e_1,e_2,\ldots,e_n) \iff \forall k,\ x_k^m = e_k \iff \forall k,\ r_k \mid m$$

The order is the minimal positive integer m satisfying this, namely $m = \operatorname{lcm}(r_1,\ldots,r_n)$. ∎

Example 4.6. Find the order of $(1,3,2,6) \in \mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_5 \times \mathbb{Z}_{20}$.
Again appealing to Corollary 3.20, the element has order

$$\operatorname{lcm}\left(\frac{4}{\gcd(1,4)}, \frac{7}{\gcd(3,7)}, \frac{5}{\gcd(2,5)}, \frac{20}{\gcd(6,20)}\right) = \operatorname{lcm}(4,7,5,10) = 140$$

[14] In this course we will only ever have *finitely many* terms in a direct product/sum: in such cases these concepts are identical for abelian groups written additively. When there are infinitely many factors, the concepts are slightly different.

When is a direct product of finite cyclic groups cyclic?

Recall that $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V$ is non-cyclic while $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ is cyclic. It is reasonable to hypothesize that the distinction is whether the orders of the components are *relatively prime.*

Corollary 4.7. *$\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic $\iff \gcd(m,n) = 1$, in which case $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.*
More generally:

- $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k} \cong \mathbb{Z}_{m_1 \cdots m_k} \iff \gcd(m_i, m_j) = 1,\ \forall i \neq j.$
- *If $n = p_1^{r_1} \cdots p_k^{r_k}$ is the prime factorization, then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$*

Proof. The generalization follows by induction on the first part.

($\Leftarrow$) If $\gcd(m,n) = 1$, then $(1,1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ has order $\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = mn$. Hence $(1,1)$ is a generator of $\mathbb{Z}_m \times \mathbb{Z}_n$, which is then *cyclic.*

($\Rightarrow$) This is an exercise.

■

Examples 4.8. 1. (Example 4.6) The group $\mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_5 \times \mathbb{Z}_{20}$ is non-cyclic since $\gcd(4,20) \neq 1$. Indeed the maximum order of an element in this group is

$$\operatorname{lcm}(4,7,5,20) = 140 < 2800 = |\mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_5 \times \mathbb{Z}_{20}|$$

2. Is $\mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{12}$ cyclic? The Corollary says yes, since none 5, 7, 12 have any common factors. It is ghastly to write, but there are 12 different ways (up to reordering) of expressing this group!

$$\begin{aligned}\mathbb{Z}_{420} &\cong \mathbb{Z}_3 \times \mathbb{Z}_{140} \cong \mathbb{Z}_4 \times \mathbb{Z}_{105} \cong \mathbb{Z}_5 \times \mathbb{Z}_{84} \cong \mathbb{Z}_7 \times \mathbb{Z}_{60} \\ &\cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_{35} \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{28} \cong \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{20} \\ &\cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{21} \cong \mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_{15} \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{12} \\ &\cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7\end{aligned}$$

We may combine/permute the factors of $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, provided we *don't separate* $2^2 = 4$.

Finite(ly generated) abelian groups

We've used the direct product to create finite abelian groups from cyclic building blocks. Our next result provides a powerful converse.

Theorem 4.9 (Fundamental Theorem of Finitely Generated Abelian Groups).
Every finitely generated[15] *abelian group is isomorphic to a group of the form*

$$\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

The p_i are (not necessarily distinct) primes, each $r_k \in \mathbb{N}$, and there are finitely many $\mathbb{Z}$-factors. A finite abelian group has no factors of $\mathbb{Z}$.

[15] Recall Exercise 3.2.11.

We won't develop the technology necessary to prove this, but it is too useful to ignore. Our purpose is simply to classify *finite abelian groups* up to isomorphism.

Examples 4.10. 1. Up to isomorphism, there are five abelian groups of order $81 = 3^4$, namely

$$\mathbb{Z}_{81}, \quad \mathbb{Z}_3 \times \mathbb{Z}_{27}, \quad \mathbb{Z}_9 \times \mathbb{Z}_9, \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9, \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

These groups can be distinguished in several ways; for instance, if G is abelian and has order 81, you could show that $G \cong \mathbb{Z}_3 \times \mathbb{Z}_{27}$ by demonstrating two facts:

- G contains an element of order 27.
- The maximum order of an element of G is 27.

2. Since $450 = 2 \cdot 3^2 \cdot 5^2$ is a prime factorization, the fundamental theorem says that every abelian group of order 450 is isomorphic to one of four groups:

(a) $\mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{5^2} \cong \mathbb{Z}_{450}$ (cyclic, max order 450)

(b) $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$ (non-cyclic, maximum order $150 = 2 \cdot 3 \cdot 5^2$)

(c) $\mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \times \mathbb{Z}_5$ (non-cyclic, maximum order $90 = 2 \cdot 3^2 \cdot 5$)

(d) $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ (non-cyclic, maximum order $30 = 2 \cdot 3 \cdot 5$)

As before, there are multiple isomorphic ways to express each group as a direct product.

We finish by listing all groups of orders 1 through 15 and abelian groups of order 16 up to isomorphism. The Fundamental Theorem gives us all the abelian groups.

order	abelian	non-abelian
1	$\mathbb{Z}_1$	
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4,\ V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$	$D_3 \cong S_3$
7	$\mathbb{Z}_7$	
8	$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$D_4,\ Q_8$
9	$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$	
10	$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$	D_5
11	$\mathbb{Z}_{11}$	
12	$\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	$D_6,\ A_4,\ Q_{12}$
13	$\mathbb{Z}_{13}$	
14	$\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$	D_7
15	$\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$	
16	$\mathbb{Z}_{16},\ \mathbb{Z}_4 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	Many

The list of non-abelian groups contains some unfamiliarity though we've met most already:

- D_n, S_3 and A_4 will be described properly in the next section.
- Q_8 is the *quaternion group* (Exercise 2.2.11), and Q_{12} a *generalized quaternion group*: look them up if interested!

There are *nine* non-isomorphic, non-abelian groups of order 16: D_8 and the direct product $\mathbb{Z}_2 \times Q_8$ are explicit examples. The table might make you suspicious that all non-abelian groups have even order: this is not so, though the smallest counter-example has order 21.

Exercises 4. Key concepts:

Direct product *Order of element via lcm* *Cyclic/gcd criteria* *Fundamental theorem*

1. List the elements of the following direct product groups:
   (a) $\mathbb{Z}_2 \times \mathbb{Z}_4$.
   (b) $\mathbb{Z}_3 \times \mathbb{Z}_3$.
   (c) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
2. Prove Theorem 4.2 by checking each of the axioms of a group.
3. Prove that $G \times H \cong H \times G$.
4. Prove that a direct product $\prod G_k$ is abelian if and only if its components G_k are all abelian.
5. Find the orders of the following elements and write down the cyclic subgroups generated by each (list all of the elements explicitly):
   (a) $(1, 3) \in \mathbb{Z}_2 \times \mathbb{Z}_4$.
   (b) $(4, 2, 1) \in \mathbb{Z}_6 \times \mathbb{Z}_4 \times \mathbb{Z}_3$.
6. Is the group $\mathbb{Z}_{12} \times \mathbb{Z}_{27} \times \mathbb{Z}_{125}$ cyclic? Explain.
7. Find a generator of the group $\mathbb{Z}_3 \times \mathbb{Z}_4$ and hence define an isomorphism $\phi : \mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$.
   (*Hint: read the proof of Corollary 4.7*)
8. State three non-isomorphic groups of order 50.
9. Suppose p, q are distinct primes. Up to isomorphism, how many abelian groups are there of order p^2q^2?
10. Complete the proof of Corollary 4.7: if $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, then $\gcd(m, n) = 1$.
    (*Hint: if* $\gcd(m, n) \geq 2$, *what is the maximum order of an element in* $\mathbb{Z}_m \times \mathbb{Z}_n$*?*)
11. Suppose G is an abelian group of order m, where m is a square-free positive integer ($\nexists k \in \mathbb{Z}_{\geq 2}$ such that $k^2 \mid m$). Prove that G is cyclic.
12. (a) Let G be a finitely generated abelian group and let H be the subset of G consisting of the identity e together with all the elements of order 2 in G. Prove that H is a subgroup of G.
    (b) In the language of the Fundamental Theorem, to which direct product is H isomorphic?
13. Suppose G is a finite abelian group and that m is a divisor of $|G|$. Prove that G has a subgroup of order m.
    (*Hint: use the the prime decomposition of m and the fundamental theorem and identify a suitable subgroup of* $\mathbb{Z}_{p_1^{r_1}} \times \cdot \times \mathbb{Z}_{p_k^{r_k}}$)

5 Permutations and Orbits

In this chapter we return to the roots of group theory and consider the re-orderings of a set.

5.1 The Symmetric Group & Cycle Notation

Definition 5.1. A *permutation* of a set A is a bijective/invertible function $\sigma : A \to A$.
The *symmetric group* S_A is the set of all permutations of A under functional composition.
The *symmetric group on n-letters*[16] S_n is the group S_A when $A = \{1, 2, \ldots, n\}$.

Examples 5.2. 1. If $A = \{1\}$, there is only one (bijective) function $A \to A$, namely the *identity function* $e : 1 \mapsto 1$. Thus S_1 has only one element and is isomorphic to $\mathbb{Z}_1$.

2. If $A = \{1, 2\}$, then there are *two* bijections $e, \mu : A \to A$:
   - $e(1) = 1$ and $e(2) = 2$ defines the identity function.
   - $\sigma(1) = 2$ and $\sigma(2) = 1$ swaps the elements of A.

$\circ$	e	σ
e	e	σ
σ	σ	e

   The Cayley table is immediate: plainly S_2 is isomorphic to $\mathbb{Z}_2$.

3. We met $S_3 = S_{\{1,2,3\}}$ explicitly in Example 1.2; it has *six elements* and is *non-abelian*, e.g.

$$\mu_1 \circ \mu_2 = \rho_1 \neq \rho_2 = \mu_2 \circ \mu_1$$

Lemma 5.3. 1. *S_A is indeed a group under composition of functions.*

2. *If A has at least three elements, then S_A is non-abelian.*
3. *The order of S_n is $n!$* *(Warning! The subscript n is not the order of S_n)*
4. *$S_m \leq S_n$ whenever $m \leq n$* *(strictly S_n contains a subgroup isomorphic to S_m)*

Proof. 1. *Closure*: If $\sigma, \tau : A \to A$ are bijective, so is the composition[17] $\sigma \circ \tau$.

Associativity: Composition of functions is associative (Theorem 2.12).

Identity: The *identity function* $e_A : a \mapsto a$ for all $a \in A$ is certainly bijective.

Inverse: If σ is a bijection, then its inverse function σ^{-1} is also bijective.

The remaining parts are exercises. ∎

From now on we simply use juxtaposition: $\sigma\tau := \sigma \circ \tau$. Remember that $\sigma\tau$ is a *function* $A \to A$, so evaluation means that we act with τ first:

$$\sigma\tau(a) = \sigma\big(\tau(a)\big)$$

Similarly, exponentiation will mean self-composition: e.g. $\sigma^3 = \sigma\sigma\sigma = \sigma \circ \sigma \circ \sigma$.

[16] Here we make S_n an *explicit* group for clarity. In practice, any set with n elements will do, and any group isomorphic to this is usually also called S_n (see Exercise 7).

[17] You should have seen this in a previous class. If you are uncomfortable with why this is true, write out the details!

Cycle Notation

Computations in S_n are facilitated by some new notation.

Definition 5.4. Suppose $\{a_1,\ldots,a_k\} \subseteq \{1,\ldots,n\}$. The *$k$-cycle* $\sigma = (a_1\, a_2 \cdots a_k) \in S_n$ is the function

$$\sigma : \begin{cases} a_j \mapsto a_{j+1} & \text{if } j < k \\ a_k \mapsto a_1 & \\ x \mapsto x & \text{if } x \notin \{a_1,\ldots,a_k\} \end{cases} \qquad a_1 \mapsto a_2 \mapsto a_3 \mapsto \cdots \mapsto a_k \qquad \text{all other } x$$

Cycles $(a_1 \cdots a_k)$ and $(b_1 \cdots b_l)$ are *disjoint* if $\{a_1,\ldots,a_k\} \cap \{b_1,\ldots,b_l\} = \emptyset$.
1-cycles and the *0-cycle* $()$ are sometimes helpful in calculations: these are simply the identity e.

Example 5.5. A 4-cycle $\sigma = (1\,3\,4\,2)$ and a 2-cycle $\tau = (1\,4)$ in S_4 are defined in the table:

x	1	2	3	4
$\sigma(x)$	3	1	4	2
$\tau(x)$	4	2	3	1

$$\sigma : 1 \mapsto 3 \mapsto 4 \mapsto 2 \qquad \tau : 1 \quad 4 \qquad 2 \quad 3$$

To compose cycles, just remember that each is a *function* and you won't go wrong!

x	1	2	3	4
$\tau(x)$	4	2	3	1
$\sigma\tau(x)$	2	1	4	3

$$\sigma\tau : 1 \quad 2 \qquad 3 \quad 4$$

The result is a product of *disjoint 2-cycles* $\sigma\tau = (1\,2)(3\,4)$.

Algorithmic Cycle Composition It is impractically slow to compute using tables. Here is an algorithmic approach that, with practice, should prove more efficient. We illustrate by verifying the previous calculation: at each step you write only a single number or bracket and thus build up the right column.

- Open a bracket and write 1: $\qquad \sigma\tau = (1$
- Since $1 \overset{\tau}{\mapsto} 4 \overset{\sigma}{\mapsto} 2$, write 2 next: $\qquad \sigma\tau = (1\,2$
- $2 \overset{\tau}{\mapsto} 2 \overset{\sigma}{\mapsto} 1$ starts the cycle; close it and open another with an unused value: $\qquad \sigma\tau = (1\,2)(3$
- $3 \overset{\tau}{\mapsto} 3 \overset{\sigma}{\mapsto} 4$, so write 4 next: $\qquad \sigma\tau = (1\,2)(3\,4$
- $4 \overset{\tau}{\mapsto} 1 \overset{\sigma}{\mapsto} 3$ starts the current cycle, so close it: $\qquad \sigma\tau = (1\,2)(3\,4)$
- All values 1, 2, 3, 4 have appeared so we terminate the algorithm.

It should be clear how to extend the algorithm when composing more cycles. If you obtain any 1-cycles, delete them. Shortly we'll prove that the algorithm always terminates in a product of disjoint cycles. For now, practice the algorithm by verifying the following:

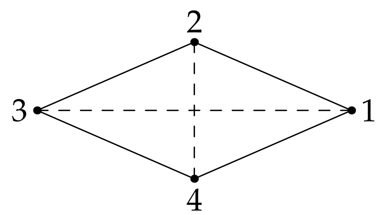
Examples 5.6. 1. $(1\,4)(1\,3\,4\,2) = (1\,3)(2\,4)$ 2. $(1\,3\,5\,4)(2\,3\,4) = (1\,3)(2\,5\,4)$

3. $(1\,2\,3\,4)(1\,2\,3)(1\,2) = (1\,4)(2\,3)$ 4. $(1\,2\,3\,4\,5\,6)^3 = (1\,4)(2\,5)(3\,6)$

Geometric Symmetry Groups

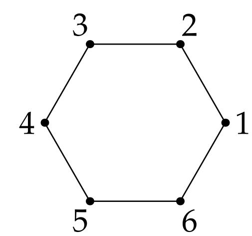
Permutations allow us to describe the group of symmetries of a geometric figure: simply label the vertices (or edges/faces) with numbers $1, 2, 3, \ldots$ and represent each rotation/reflection by how it permutes these values. Cycle notation makes calculating compositions of symmetries easy!

Examples 5.7. 1. Label the vertices of a rhombus to view the Klein four-group V as a subgroup of S_4: the 2-cycles $(1\,3)$ and $(2\,4)$ are *reflections*, and their composition is *rotation* by 180°.



$$V \cong \{e, (1\,3), (2\,4), (1\,3)(2\,4)\}$$

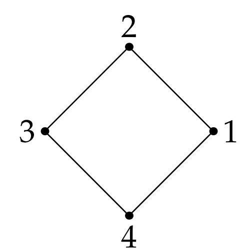
2. Label the vertices of a regular hexagon 1 through 6.



   - The 2,2-cycle $(1\,5)(2\,4)$ represents reflection across the axis through 3 and 6.
   - The 6-cycle $(1\,2\,3\,4\,5\,6)$ represents a one-step counter-clockwise rotation.

   Both are therefore identified with elements of the dihedral group D_6.

3. By labelling the vertices of a square as shown, we identify D_4 with a subgroup of S_4. All elements and the complete subgroup diagram are given below, where we follow the convention to denote reflections across diagonals (δ_j) and the midpoints of sides (μ_j) differently.



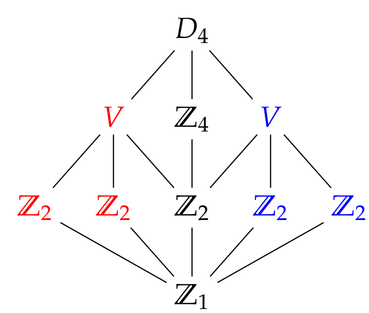
   Cycle notation makes calculation easy: for instance

$$(2\,4)(1\,2)(3\,4) = (1\,4\,3\,2) \implies \delta_1\mu_1 = \rho_3$$

   That two reflections make a rotation is geometrically obvious, but identifying *which* rotation is harder without the the ability to calculate!

	Element	Cycle notation
Rotations	ρ_0	$e = ()$
	ρ_1	(1234)
	ρ_2	$(13)(24)$
	ρ_3	(1432)
Reflections	μ_1	$(12)(34)$
	μ_2	$(14)(23)$
	δ_1	(24)
	δ_2	(13)

Subgroup	Isomorph
$\{\rho_0\}$	$\mathbb{Z}_1$
$\{\rho_0, \mu_i\}$	$\mathbb{Z}_2$
$\{\rho_0, \delta_i\}$	$\mathbb{Z}_2$
$\{\rho_0, \rho_2\}$	$\mathbb{Z}_2$
$\{\rho_0, \rho_1, \rho_2, \rho_3\}$	$\mathbb{Z}_4$
$\{\rho_0, \mu_1, \mu_2, \rho_2\}$	V
$\{\rho_0, \delta_1, \delta_2, \rho_2\}$	V



   You should be able to recognize these subgroups geometrically; e.g. the blue copy of V is precisely that in the first example. Also try to convince yourself why there are no other subgroups.

The same sort of thing can be done for 3D figures like the tetrahedron (see Section 5.3).

Cayley's Theorem

In mathematics, the word *group* originally referred to a set of permutations. We finish this section with a foundational result: every element of a group may be viewed as a permutation of the group itself, thus linking to the original meaning of the word.

Theorem 5.8 (Cayley). *Every group is isomorphic to a group of permutations.*

Proof. Let G be a group. For each $a \in G$, let $\sigma_a : G \to G$ be left multiplication by a, i.e. $\sigma_a(x) = ax$. We claim that the set of such functions $\{\sigma_a : a \in G\}$ forms a subgroup of S_G isomorphic to G.
First observe that σ_a has inverse function $\sigma_a^{-1} = \sigma_{a^{-1}}$, since

$$\forall x \in G, \quad \sigma_{a^{-1}}\big(\sigma_a(x)\big) = a^{-1}ax = x \quad \text{and} \quad \sigma_a\big(\sigma_{a^{-1}}\big)(x) = aa^{-1}x = x$$

It follows that each σ_a is a permutation of G: that is $\sigma_a \in S_G$.
We finish by showing that the function $\phi : G \to \{\sigma_a : a \in G\}$ defined by $\phi(a) = \sigma_a$ is an isomorphism:

Injectivity: $\phi(a) = \phi(b) \implies \sigma_a = \sigma_b \implies a = \sigma_a(e) = \sigma_b(e) = b$.

Surjectivity: Certainly every function σ_a is in the range of ϕ!

Homomorphism: For all $a, b, x \in G$,

$$\big(\phi(a) \circ \phi(b)\big)(x) = \sigma_a\big(\sigma_b(x)\big) = abx = \sigma_{ab}(x) = \big(\phi(ab)\big)(x)$$

from which $\phi(a) \circ \phi(b) = \phi(ab)$.

■

Cayley's Theorem *does not* say that every group is isomorphic to some symmetric group. It says that that every group G is isomorphic to *a subgroup* of S_G.

Exercises 5.1. Key concepts:

Permutation *Symmetric group* *Cycle notation*

1. Which of the following functions are permutations? Explain.
   (a) $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x) = x - 7$.
   (b) $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x) = -3x + 4$.
   (c) $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^3 - x$.
   (d) $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^3 + x$.
   (e) $f : \{\text{fish, horse, dog, cat}\} \to \{\text{fish, horse, dog, cat}\}$ where

$$f : \begin{pmatrix} \text{fish} \\ \text{horse} \\ \text{dog} \\ \text{cat} \end{pmatrix} = \begin{pmatrix} \text{horse} \\ \text{cat} \\ \text{dog} \\ \text{fish} \end{pmatrix}$$

2. Compute the following products of permutations in cycle notation.

   (a) $(1\,2)(3\,4)(1\,2\,3) \in S_4$

   (b) $(1\,4)(2\,3)(3\,4)(1\,4) \in S_4$

   (c) $(1\,2\,3)(2\,3\,4)(3\,4\,1)(4\,1\,2) \in S_4$

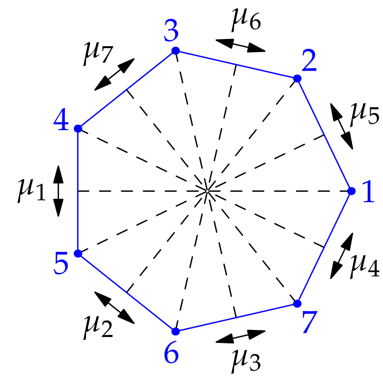
   (d) $(1\,2\,4\,5)^2(2\,4\,5)^2 \in S_5$

3. Consider the dihedral group D_7 of symmetries of the regular heptagon, viewed as a subgroup of S_7. Each μ_i is reflection across the indicated dashed line, and ρ_j is rotation j steps counter-clockwise.

   (a) State μ_4 in cycle notation.

   (b) Compute $\mu_3\rho_1$ using cycle notation. What element of D_7 does this represent?

   (c) Calculate $(\rho_2\mu_3\rho_1)^{666}$.



$\rho_1 = (1\,2\,3\,4\,5\,6\,7),\ \rho_j = \rho_1^j$

4. State the elements of the rotation group R_5 in cycle notation when viewed as a subgroup of S_5.

5. Prove parts 2, 3, and 4 of Lemma 5.3.

6. How many distinct subgroups of S_4 are isomorphic to S_3. Describe them.

7. Suppose sets A and B have the same cardinality: that is, $\exists \mu : A \to B$ bijective.

   (a) If $\sigma \in S_A$ is a permutation, show that $\mu\sigma\mu^{-1} \in S_B$.

   (b) Hence prove that S_A and S_B are isomorphic.

8. Cayley's Theorem says that G is isomorphic to a subgroup of S_G. What can you say about a finite group G if $G \cong S_G$?

9. In Cayley's theorem we defined $\sigma_a : G \to G$ via *left multiplication.*

   (a) Does the argument still work if $\sigma_a : G \to G$ is *right multiplication* $\sigma_a(x) = xa$?

   (b) (Harder) Suppose we take $\sigma_a(x) := axa^{-1}$. Where does the proof of Cayley's Theorem fail?

10. Show that the group S_3 is indecomposable: there are no groups G, H of order less than $|S_3|$ for which $S_3 \cong G \times H$.

    (*Hint: Assuming S_3 is decomposable, there is only one possible decomposition. Why does this decomposition make no sense?*)

11. Let $n \geq 3$. Prove that if $\sigma \in S_n$ commutes with every other element of S_n (i.e. $\sigma\rho = \rho\sigma$, $\forall \rho \in S_n$) then σ is the identity.

    (*Hint: suppose $\sigma(a) = b \neq a$ and consider the cases $\sigma(b) = a$ and $\sigma(b) \neq a$ separately*)

5.2 Orbits

In this section we begin to consider the idea of a *group action*; how the elements of a group transform a set. We've already seen examples of this; for instance how rotations transform an object. The simplest general example is built into the definition of the symmetric group and appears naturally in cycle notation.

Definition 5.9. The *orbit* of $\sigma \in S_n$ containing $x \in \{1, 2, \ldots, n\}$ is the *set*

$$\mathrm{orb}_x(\sigma) = \{\sigma^k(x) : k \in \mathbb{Z}\} \subseteq \{1, 2, \ldots, n\}$$

Warning! Each orbit is a subset of $\{1, 2, \ldots, n\}$, *not* of the group S_n.
Observe also that $\mathrm{orb}_{\sigma^k(x)}(\sigma) = \mathrm{orb}_x(\sigma)$ for *any* $k \in \mathbb{Z}$.

Examples 5.10. If $\sigma \in S_n$ is written as a product of *disjoint cycles*, then the cycles are the orbits!

1. The orbits of $(1\,3\,4) \in S_4$ are the disjoint sets $\{1, 3, 4\}, \{2\}$.
2. The orbits of $(1\,2)(4\,5)$ are $\{1, 2\}, \{3\}, \{4, 5\}$.
3. This is *false* if the cycles are not disjoint. For instance, $\sigma = (1\,3)(2\,3\,4) \in S_4$ maps

   $$1 \mapsto 3 \mapsto 4 \mapsto 2 \mapsto 1$$

   so there is only one orbit: $\mathrm{orb}_x(\sigma) = \{1, 2, 3, 4\}$ for any x. This comports with the result $\sigma = (1\,2\,3\,4)$ of multiplying out σ using our algorithm.

Given that disjoint cycle notation is so useful for reading orbits, it is natural to ask if *any* permutation can be written as a product of disjoint cycles. The answer is yes, and the disjoint cycles turn out to be precisely the orbits!

Theorem 5.11. *The orbits of any $\sigma \in S_n$ partition $X = \{1, 2, \ldots, n\}$.*

Proof. Define a relation $\sim$ on $X = \{1, 2, \ldots, n\}$ by $x \sim y \iff y \in \mathrm{orb}_x(\sigma)$. We claim that this is an equivalence relation.[18]

Reflexivity $x \sim x$ since $x = \sigma^0(x)$. ✓

Symmetry $x \sim y \implies y = \sigma^k(x)$ for some $k \in \mathbb{Z}$. But then $x = \sigma^{-k}(y) \implies y \sim x$. ✓

Transitivity Suppose that $x \sim y$ and $y \sim z$. Then $y = \sigma^k(x)$ and $z = \sigma^l(y)$ for some $k, l \in \mathbb{Z}$. But then $z = \sigma^{k+l}(x)$ and so $x \sim z$. ✓

The equivalence classes of $\sim$ are clearly the orbits of σ, which therefore partition X. ∎

[18] If $\sim$ is a relation on a set X and $x \in X$, we may define the set $[x] := \{y \in X : y \sim x\}$. In this case $[x] = \mathrm{orb}_x(\sigma)$.

Theorem: The sets $[x]$ *partition* X (every $y \in X$ lies in precisely one such subset $[x]$) if and only if $\sim$ is an *equivalence relation* (reflexive, symmetric, transitive). In such a case we call $[x]$ an *equivalence class*.

Much of the rest of the course requires these crucial ideas. If they're not familiar, review your notes from a previous class and ask questions!

Theorem 5.12. *Every permutation can be written as a product of disjoint cycles.*

Proof. We formalize our algorithm from the previous section. Suppose $\sigma \in S_n$ is given.

1. List the elements of $\text{orb}_1(\sigma)$ in the order they appear within the orbit:

   $$\text{orb}_1(\sigma) = \{1, \sigma(1), \sigma^2(1), \ldots\}$$

   If this all of $X = \{1, \ldots, n\}$, we are finished: $\sigma = \big(1\ \sigma(1)\ \sigma^2(1)\ \ldots\ \sigma^{n-1}(1)\big)$ is an n-cycle.
2. Otherwise, let $x_2 = \min\{x \in X : x \notin \text{orb}_1(\sigma)\}$ and construct its orbit:

   $$\text{orb}_{x_2}(\sigma) = \{x_2, \sigma(x_2), \sigma^2(x_2), \ldots\}$$

   By Theorem 5.11, $\text{orb}_{x_2}(\sigma)$ is disjoint with $\text{orb}_1(\sigma)$. If $\text{orb}_1(\sigma) \cup \text{orb}_{x_2}(\sigma) = X$, we are finished: σ is the product of two disjoint cycles.

   $$\sigma = \big(1\ \sigma(1)\ \sigma^2(1)\ \cdots\big)\big(x_2\ \sigma(x_2)\ \sigma^2(x_2)\ \cdots\big)$$

3. Otherwise, we repeat. At stage k, let $x_k = \min\{x \in X : x \notin \text{orb}_1(\sigma) \cup \cdots \cup \text{orb}_{k-1}(\sigma)\}$. By the Theorem, $\text{orb}_{x_k}(\sigma)$ is disjoint with $\text{orb}_1(\sigma) \cup \cdots \cup \text{orb}_{k-1}(\sigma)$. The process continues until $\text{orb}_1(\sigma) \cup \cdots \cup \text{orb}_k(\sigma) = X$, which must happen since X is a finite set. The result is a product of disjoint cycles:

   $$\sigma = \underbrace{\big(1\ \sigma(1)\ \sigma^2(1)\ \cdots\big)}_{\text{orb}_1(\sigma)}\underbrace{\big(x_2\ \sigma(x_2)\ \sigma^2(x_2)\ \cdots\big)}_{\text{orb}_{x_2}(\sigma)}\underbrace{\big(\cdots\cdots\big)}_{\text{orb}_{x_3}(\sigma)}\cdots\underbrace{\big(\cdots\cdots\big)}_{\text{orb}_{x_k}(\sigma)}$$ ∎

The Theorem explains why our algorithm always results in a product of disjoint cycles! By convection, we take $x_1 = 1$ and construct an increasing sequence $x_1 \le x_2 \le \cdots \le x_k$, though there is no need to do so: disjoint cycles can be listed in any order and may start with any element, thus

$$(1\,3)(2\,5\,4) = (5\,4\,2)(3\,1)$$

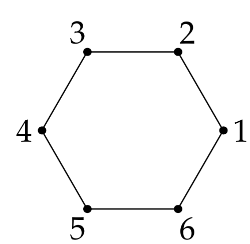
Also, by convention, we delete any orbits of size 1 (1-cycles). If you are still feeling uncomfortable multiplying cycles, practice until it becomes second-nature!

Orders of Elements in S_n

Recall that the order of an element σ is the least positive integer k for which $\sigma^k = e$.

Example 5.13. If $\sigma = (1\,2\,3\,4\,5\,6) \in S_6$, then

$$\sigma^2 = (1\,3\,5)(2\,4\,6) \qquad \sigma^3 = (1\,4)(2\,5)(3\,6) \qquad \sigma^4 = (1\,5\,3)(2\,6\,4)$$
$$\sigma^5 = (1\,6\,5\,4\,3\,2) \qquad \sigma^6 = e$$



whence the order of σ is 6. This follows intuitively if we identify σ with a rotation of a regular hexagon.

By thinking similarly about the regular k-gon, it should be clear that any k-cycle has order k.

Things are trickier when you don't have a single cycle, though this is where our discussion of disjoint cycles saves us, since *disjoint cycles commute.*

Examples 5.14. 1. Since $(1\,2\,3)$ and $(4\,5)$ are disjoint cycles, we know that $(1\,2\,3)(4\,5) = (4\,5)(1\,2\,3)$. We therefore easily compute the following:

$$\begin{aligned}\big((1\,2\,3)(4\,5)\big)^3 &= (1\,2\,3)(4\,5)(1\,2\,3)(4\,5)(1\,2\,3)(4\,5) \\ &= (1\,2\,3)^3(4\,5)^3 = e(4\,5) = (4\,5)\end{aligned}$$

2. Given $\sigma = (2\,5\,3)(1\,5\,4\,3) \in S_5$, find σ^8. It is *really* tempting to write

$$\sigma^8 \stackrel{?}{=} (2\,5\,3)^8(1\,5\,4\,3)^8 = \big((2\,5\,3)^3\big)^2(2\,5\,3)^2\big((1\,5\,4\,3)^4\big)^2 = e^3(2\,3\,5)e^2 = (2\,3\,5)$$

but this is incorrect. The *cycles don't commute* $(2\,5\,3)(1\,5\,4\,3) \neq (1\,5\,4\,3)(2\,5\,3)$ so we can't distribute the exponent. Instead we first write σ as a product of disjoint cycles, then

$$\sigma = (1\,3)(2\,5\,4) \implies \sigma^8 = (1\,3)^8(2\,5\,4)^8 = (2\,5\,4)^2 = (2\,4\,5)$$

The disjoint cycles approach also tells us the *order* of σ. Observe that

$$e = \sigma^k = (1\,3)^k(2\,5\,4)^k \iff k \text{ is divisible by both 2 and 3}$$

The order if σ is therefore 6.

Corollary 5.15. *The order of a permutation σ is the least common multiple of the lengths of its disjoint cycles.*

Proof. Write $\sigma = \sigma_1 \cdots \sigma_m$ as a product of disjoint cycles. Since these commute, we have

$$\sigma^k = \sigma_1^k \cdots \sigma_m^k$$

Since each factor σ_j^k permutes disjoint sets, it follows that

$$\sigma^k = e \iff \forall j,\ \sigma_j^k = e$$

If the orbits of σ have lengths $r_j \in \mathbb{N}$, it follows that

$$\sigma_j^k = e \iff \alpha_j \mid k$$

Thus k must be a multiple of α_j for all j. The least such k is by definition $\operatorname{lcm}(\alpha_1, \ldots, \alpha_m)$. ∎

Example 5.16. The order of $\sigma = (1\,4\,5)(3\,6\,2\,7)(8\,9) \in S_9$ is $\operatorname{lcm}(3,4,2) = 12$.
To find σ^{3465}, first observe that $3465 = 12 \cdot 288 + 9$, whence

$$\sigma^{3465} = (\sigma^{12})^{288}\sigma^9 = \sigma^9 = (1\,4\,5)^9(3\,6\,2\,7)^9(8\,9)^9 = (3\,6\,2\,7)(8\,9)$$

since $(1\,4\,5)$, $(3\,6\,2\,7)$ and $(8\,9)$ have orders 3, 4 and 2 respectively.

Exercises 5.2. Key concepts:

Orbit *Partition* *Disjoint cycles* *Order of element via lcm*

1. Find the orbits of the following permutations, and their orders:
   (a) $\rho = (1\,4\,5)(2\,3\,4\,5) \in S_5$.
   (b) $\sigma = (1\,5\,4)(2\,5\,4)(1\,2\,3\,4) \in S_5$.
   (c) $\tau = (1\,5\,7\,4)(3\,2\,4)(3\,2\,5\,6) \in S_7$.
2. If $\sigma \in S_A$ is any permutation, we may define its orbits similarly: $\mathrm{orb}_a(\sigma) = \{\sigma^j(a) : j \in \mathbb{Z}\}$. What are the orbits of the permutation $\sigma : \mathbb{Z} \to \mathbb{Z} : n \mapsto n+3$?
3. Given $\sigma = (1\,3)(2\,4\,5) \in S_5$, find the elements of the cyclic group $\langle \sigma \rangle \leq S_5$ generated by σ.
4. What is the largest possible order of an element of the group $S_3 \times \mathbb{Z}_4 \times V$? Exhibit one.
5. What is the maximum order of an element in each of the groups S_4, S_5, S_6, S_7, S_8? Exhibit a maximum order element in each case.
6. For which integers n does there exist a subgroup $C_n \leq S_8$ where C_n is cyclic of order n? Explain your answer.
7. Let $\sigma \in S_n$. For each $k > 0$, prove that each orbit of σ^k is a subset of an orbit of σ.
8. Consider the permutations $\sigma = (1\,3\,5)(2\,7\,4\,9\,6)$ and $\tau = (1\,5\,3\,2)(6\,9)$ in S_9.
   (a) Compute $\sigma\tau$ and $\tau\sigma$ in cycle notation.
   (b) Find the orders of σ, τ, $\sigma\tau$ and $\tau\sigma$.
   (c) Compute $(\sigma\tau)^{432}\sigma^{43}$ as a product of disjoint cycles.
   (d) Construct the subgroup diagram of $\langle \sigma \rangle$ and give a generator for each subgroup.

5.3 Transpositions & the Alternating Group

Instead of breaking a permutation σ into disjoint cycles, we can consider a permutation as constructed from only the simplest bijections.

Definition 5.17. A 2-cycle $(a_1\, a_2)$ is also known as a *transposition*, since it swaps two elements of $\{1, 2, \dots, n\}$ and leaves the rest untouched.

Theorem 5.18. *Every $\sigma \in S_n$ ($n \geq 2$) is the product of transpositions.*

Proof. There are many, many ways to write out a single permutation as a product of transpositions. One method is first to write σ as a product of disjoint cycles, then write each cycle as follows:

$$(a_1\ \cdots\ a_k) = (a_1\, a_k)(a_1\, a_{k-1}) \cdots (a_1\, a_2)$$

Just read it carefully and you should be convinced this works! ∎

Example 5.19. The method in the proof results in the decomposition

$$(1\,7\,6\,4\,5) = (1\,5)(1\,4)(1\,6)(1\,7)$$

Other decompositions are possible, for instance $(1\,7)(3\,6)(5\,7)(4\,7)(3\,6)(6\,7)$.

While there are many ways to write a permutation as a product of transpositions, there is a simple commonality which can be observed via a *matrix notation* for permutations. Consider, for instance,

$$\begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix}\begin{pmatrix}1\\2\\3\\4\end{pmatrix} = \begin{pmatrix}1\\4\\3\\2\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}0&0&1&0\\0&0&0&1\\0&1&0&0\\1&0&0&0\end{pmatrix}\begin{pmatrix}1\\2\\3\\4\end{pmatrix} = \begin{pmatrix}3\\4\\2\\1\end{pmatrix} \tag{$*$}$$

Each 4×4 matrix *permutes* the values $1, 2, 3, 4$ when placed in a column vector. These matrices plainly correspond to the transposition $(2\,4)$ and the 4-cycle $(1\,3\,2\,4)$ in S_4.

Definition 5.20. An $n \times n$ *permutation matrix* is a matrix obtained from the identity matrix by permuting its *rows*. Equivalently, it is zero except for a single 1 in each row and column.

Lemma 5.21. *The set of $n \times n$ permutation matrices forms a group under multiplication which is isomorphic to S_n.*

We omit a formal proof, though it relies on essentially one fact from elementary linear algebra; that *row operations* preserve the solution set of a system of linear equations. For instance $(*)$ describes two systems $A\mathbf{x} = \mathbf{b}$ and $C\mathbf{x} = \mathbf{d}$ which are identical up to rearrangements of rows (row operations) and moreover have identical solutions $\mathbf{x} = \left(\begin{smallmatrix}1\\2\\3\\4\end{smallmatrix}\right)$.

What does this have to do with transpositions? Since a transposition swaps two elements, it corresponds to an *elementary matrix* which swaps two rows; such a matrix always has determinant -1. Suppose that a permutation is written as a product of transpositions:

$$\sigma = \sigma_1 \cdots \sigma_m$$

Viewing this as a product of matrices, take the determinant of both sides to observe that

$$\det \sigma = (-1)^m$$

Notice that this depends only on whether m is *even* or *odd*...

Definition 5.22. A permutation $\sigma \in S_n$ is *even/odd* if it can be written as the product of an even/odd number of transpositions. By the above discussion, these concepts are well-defined: a permutation is *either* even or odd; it cannot be both!

Plainly the composition of even permutations remains even, as does the inverse of such. We may therefore define a new subgroup of S_n.

Definition 5.23. The *alternating group* A_n ($n \geq 2$) is the group of even permutations in S_n.

Theorem 5.24. *A_n has exactly half the elements of S_n: that is $|A_n| = \frac{n!}{2}$.*

Proof. Since $n \geq 2$, we have $(1\,2) \in S_n$. Define $\phi : S_n \to S_n$ by $\phi(\sigma) = (1\,2)\sigma$. Since

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

we see that ϕ is invertible: the inverse of ϕ is ϕ itself! Moreover, ϕ maps even permutations to odd and vice versa. It follows that there are exactly the same number of odd and even permutations. ■

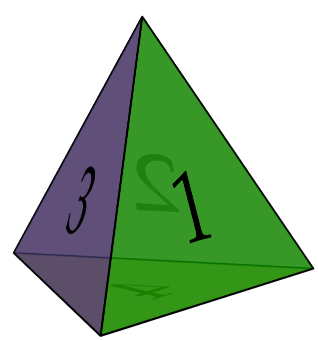
Examples 5.25. We describe the small alternating groups up to A_4.

1. $A_2 = \{e\} \cong \mathbb{Z}_1$ is extremely boring!
2. $A_3 = \{e, (1\,3)(1\,2), (1\,2)(1\,3)\} = \{e, (1\,2\,3), (1\,3\,2)\} \cong \mathbb{Z}_3$ is a cyclic group.
3. When $n = 4$ we obtain the first 'new' group in the alternating family; a group of order 12.

$$A_4 = \{e, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3), \\ (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

A_4 is non-abelian: for example,

$$(1\,2\,3)(1\,2\,4) = (1\,3)(2\,4) \neq (1\,4)(2\,3) = (1\,2\,4)(1\,2\,3)$$



We already know one non-abelian group of order 12: the dihedral group D_6. We quickly see that $A_4 \not\cong D_6$: all elements of A_4 have orders 1, 2 or 3, while D_6 contains a rotation of order 6.

By labelling faces (or vertices), A_4 may be visualized the rotation group of the tetrahedron: can you see how each element acts?

Exercises 5.3. Key concepts:

Transposition (representation by) *Odd/even permutations* *Alternating group*

1. Write $(1\,3\,4\,6)(2\,4\,6)$ as a product of transpositions in two different ways.
2. State $\sigma = (1\,3)$ and $\tau = (1\,3\,2)$ as 3×3 permutation matrices S and T. Compute the matrix product ST and verify that it is the permutation matrix corresponding to $\sigma\tau \in S_3$.
3. Give examples of two non-isomorphic non-abelian groups of order 360.
4. Explain why every finite group is isomorphic to a group of matrices under multiplication.
5. S_4 has *four* distinct subgroups isomorphic to the Klein four-group V; state them. Only one of these is a subgroup of A_4; which?
6. We just saw that the rotation group of a regular tetrahedron is isomorphic to A_4.
   (a) What is the order of the rotation group of a cube?
   (*Hint: each face may be rotated to any of six faces, and then rotated in place...*)
   (b) Repeat the calculation for the remaining three platonic solids (octahedron, dodecahedron, icosahedron).
   (c) By placing a vertex at the center of each face of a cube, argue that the rotation group of an octahedron is also isomorphic to S_4.
   What happens when you do this for a dodecahedron? A tetrahedron?
   (d) Label the four diagonals of a cube 1, 2, 3, 4. Describe geometrically the effect of the permutation $(2\,3\,4)$ on the cube. What about $(2\,3)$? Hence conclude that the rotation group of a cube is isomorphic to S_4.
   (*The dodecahedral and icosahedral rotation groups are both isomorphic to the alternating group A_5, though this is harder to visualize than the cube situation—try researching a proof*)
7. (Hard) Find the entire subgroup diagram of A_4.
8. (Hard) Prove that D_n is a subgroup of $A_n \iff n \equiv 1 \pmod 4$
   (*Do this in one shot if you like; otherwise use the following steps to guide your thinking*)
   (a) Label the corners of a regular n-gon 1 through n counter-clockwise so that every element of D_n may be written as a permutation of $\{1, 2, \ldots, n\}$. Write in a sentence what you are required to prove: what condition characterizes being in the group A_n?
   (b) Consider the rotation $\rho_1 = (1\,2\,3\,\cdots\,n)$ of the n-gon one step counter-clockwise. Is ρ_1 odd or even, and how does this depend on n?
   (c) Show that every rotation $\rho_i \in D_n$ is generated by ρ_1. When is the set of rotations in D_n a subgroup of A_n?
   (d) A reflection $\mu \in D_n$ permutes corners of the n-gon by swapping pairs. How many pairs of corners does μ swap when $n \equiv 1 \pmod 4$? Is μ an odd or even permutation? You may use a picture, provided it is sufficiently general.
   (e) Summarize parts (a–d) to argue the $\Leftarrow$ direction of the theorem.
   (f) Prove the $\Rightarrow$ direction of the theorem by exhibiting an element of D_n which is not in A_n whenever $n \not\equiv 1 \pmod 4$.

6 Cosets & Factor Groups

In this chapter[19] we partition a group into subsets so that the *set of subsets* inherits a natural group structure. This will likely feel extremely abstract and difficult. However, it is really nothing new; it is precisely the idea behind modular arithmetic.

Example 6.1. In $\mathbb{Z}_3 = \{0, 1, 2\}$ the elements are really *subsets* $[0], [1], [2]$ of the *integers* $\mathbb{Z}$:

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv 0 \pmod 3\} = \{\ldots, -3, 0, 3, 6, \ldots\} \\
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\} = \{\ldots, -2, 1, 4, 7, \ldots\} \\
[2] &= \{x \in \mathbb{Z} : x \equiv 2 \pmod 3\} = \{\ldots, -1, 2, 5, 8, \ldots\}
\end{aligned}$$

When we write $1 +_3 2 = 0 \in \mathbb{Z}_3$, we really mean

$$\forall x \in [1], y \in [2] \text{ we have } x + y \in [0]$$

Addition on $\mathbb{Z}$ naturally induces addition modulo 3 on the set of subsets $\mathbb{Z}_3 = \{[0], [1], [2]\}$.

6.1 Cosets & Normal Subgroups

Our main goal is to generalize the example. Start by observing that the identity element $[0]$ is a *subgroup* of $\mathbb{Z}$ from which the sets $[1]$, $[2]$ may be obtained by *translation.*

Definition 6.2. Let H be a subgroup of G and $g \in G$. The *left coset* of H containing g is

$$gH := \{gh : h \in H\} \qquad (x \in gH \iff \exists h \in H \text{ such that } x = gh)$$

This is a subset of G. The *right coset* of H containing g is defined similarly:

$$Hg := \{hg : h \in H\}$$

The *identity coset* $H = eH = He$ is the left & right coset of H containing the identity e.
H is a *normal subgroup* of G, written $H \triangleleft G$, if the left and right cosets containing g are always equal

$$H \triangleleft G \iff \forall g \in G,\ gH = Hg$$

If G is written additively, then the left and right cosets of H containing g are instead written

$$g + H := \{g + h : h \in H\} \qquad H + g := \{h + g : h \in H\}$$

Example (6.1 cont). Let $G = \mathbb{Z}$ and $H = [0] = 3\mathbb{Z}$. The left and right cosets of H are precisely the elements of $\mathbb{Z}_3$:

$$\begin{aligned}
3\mathbb{Z} = 0 + 3\mathbb{Z} = 3\mathbb{Z} + 0 &= [0] = \{\ldots, -3, 0, 3, 6, \ldots\} \\
1 + 3\mathbb{Z} = 3\mathbb{Z} + 1 &= [1] = \{\ldots, -2, 1, 4, 7, \ldots\} \\
2 + 3\mathbb{Z} = 3\mathbb{Z} + 2 &= [2] = \{\ldots, -1, 2, 5, 8, \ldots\}
\end{aligned}$$

Since the left and right cosets are equal, $H = 3\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$.

[19]The examples are everything in this chapter: write everything out by hand until it becomes easy—there is no shortcut!

The last observation is in fact general—we leave the proof as a straightforward exercise.

Lemma 6.3. *Every subgroup of an abelian group G is normal.*

For non-abelian groups, most subgroups are typically *not* normal: see Example 6.4.2 below.

Examples 6.4. 1. Consider the subgroup $H = \langle 4 \rangle = \{0, 4, 8\} \leq \mathbb{Z}_{12}$. This is cyclic with order 3. The distinct cosets of $\langle 4 \rangle$ are as follows (left = right since $\mathbb{Z}_{12}$ is abelian!):

$$\begin{aligned} \langle 4 \rangle &= \{0,4,8\} && (= 4 + \langle 4 \rangle = 8 + \langle 4 \rangle) \\ 1 + \langle 4 \rangle &= \{1,5,9\} && (= 5 + \langle 4 \rangle = 9 + \langle 4 \rangle) \\ 2 + \langle 4 \rangle &= \{2,6,10\} && (= 6 + \langle 4 \rangle = 10 + \langle 4 \rangle) \\ 3 + \langle 4 \rangle &= \{3,7,11\} && (= 7 + \langle 4 \rangle = 11 + \langle 4 \rangle) \end{aligned}$$

Observe that the cosets *partition* $\mathbb{Z}_{12}$ into equal-sized subsets.

2. By revisiting the multiplication table for D_3 (Example 1.2) or using cycle notation, we verify that the left and right cosets of the subgroup $H = \{e, \mu_1\}$ are as follows:

Left cosets	Right cosets
$H = \mu_1 H = \{e, \mu_1\}$	$H = H\mu_1 = \{e, \mu_1\}$
$\rho_1 H = \mu_3 H = \{\rho_1, \mu_3\}$	$H\rho_1 = H\mu_2 = \{\rho_1, \mu_2\}$
$\rho_2 H = \mu_2 H = \{\rho_2, \mu_2\}$	$H\rho_2 = H\mu_3 = \{\rho_1, \mu_3\}$

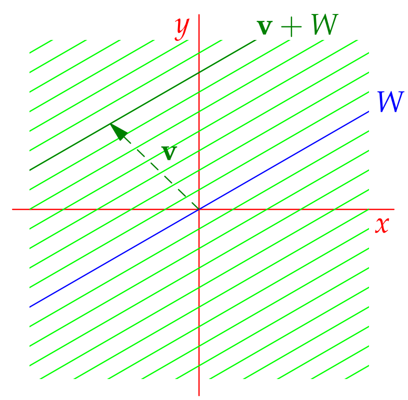
This time the left and right cosets of H are not all the same: H is *not* a normal subgroup of D_3. The partitioning observation still holds: the left cosets partition D_3 into three equal-sized subsets; the right cosets also partition into equal-sized subsets, just different ones.

3. Consider a 1-dimensional subspace $W \leq \mathbb{R}^2$; this is a line through the origin. The coset

$$\mathbf{v} + W = \{\mathbf{v} + \mathbf{w} : \mathbf{w} \in W\}$$

is a line parallel to W. The cosets thus comprise all lines parallel to W. Note again that these *partition* $\mathbb{R}^2$: every point in $\mathbb{R}^2$ lies in precisely one coset.

More generally, if W is a subspace of a vector space V, then the cosets $\mathbf{v} + W$ are the sets parallel to W. Only the zero coset $W = \mathbf{0} + W$ is a sub*space*.



4. Recall Theorem 5.24. If we generalize the argument, we see that, for any $\alpha \in A_n$ and $\sigma \in S_n$,

$$\alpha\sigma \text{ even} \iff \sigma \text{ even} \iff \sigma\alpha \text{ even}$$

Otherwise said, for any $\sigma \in S_n$, the cosets of A_n containing σ are

$$\sigma A_n = A_n \sigma = \begin{cases} A_n & \text{if } \sigma \text{ even} \\ B_n & \text{if } \sigma \text{ odd} \end{cases}$$

where B_n is the set of odd permutations in S_n. In particular, A_n is a normal subgroup of S_n.

As observed in the examples, the cosets of any subgroup $H \leq G$ seem to partition G.

Theorem 6.5. *Let H be a subgroup of G. Then the left cosets of H partition G. Moreover,*

$$y \in xH \iff x^{-1}y \in H \iff xH = yH$$

The right cosets partition G similarly: indeed

$$y \in Hx \iff yx^{-1} \in H \iff Hx = Hy$$

The blue criterion is particularly useful as it is often very easy to check. Before reading the proof, convince yourself that each previous example satisfies the result. When H is non-normal (e.g. Example 2), the right cosets partition G in a *different way* to the left cosets!

Proof. We start by verifying the first connective.

$$y \in xH \iff \exists h \in H \text{ such that } y = xh \iff x^{-1}y = h \in H$$

Now define a relation $\sim$ on G via $x \sim y \iff y \in xH$. We claim this is an equivalence relation:

Reflexivity: $x \sim x$ since $x^{-1}x = e \in H$.

Symmetry: $x \sim y \implies x^{-1}y \in H \implies (x^{-1}y)^{-1} \in H$, since H is a subgroup. But then

$$y^{-1}x \in H \implies y \sim x$$

Transitivity: If $x \sim y$ and $y \sim z$ then $x^{-1}y \in H$ and $y^{-1}z \in H$. But H is closed, whence

$$x^{-1}z = (x^{-1}y)(y^{-1}z) \in H \implies x \sim z$$

The equivalence classes therefore partition G. Since $x \sim y \iff y \in xH$, the equivalence class of x is indeed the left coset xH, as required. ∎

It is precisely the fact that H is a subgroup which guarantees a partition (compare Theorem 2.19)!

Reflexivity: H contains the identity (and is thus non-empty).

Symmetry: H satisfies the inverse axiom.

Transitivity: H is closed under the group operation.

When H is not a subgroup, the coset construction is unlikely to produce a partition.

Example 6.6. The *subset* $H = \{0, 1\} \subseteq \mathbb{Z}_3$ is not a subgroup. Its left 'cosets' fail to partition $\mathbb{Z}_3$:

$$H = \{0, 1\}, \quad 1 + H = \{1, 2\}, \quad 2 + H = \{2, 1\}$$

We finish this section with a technical result which will be useful in future sections.

Corollary 6.7. *Normal subgroups are precisely those which are closed under* conjugation*:*

$$H \triangleleft G \iff \forall g \in G,\ h \in H,\ \text{we have } ghg^{-1} \in H$$

Proof. Start by using the above criteria to observe:

(a) $gH \subseteq Hg \iff \forall h \in H,\ gh \in Hg \iff \forall h \in H,\ ghg^{-1} \in H$

(b) $Hg \subseteq gH \iff \forall h \in H,\ hg \in gH \iff \forall h \in H,\ g^{-1}hg \in H$

We may now complete the proof in two parts:

($\Rightarrow$) $H \lhd G \implies$ part (a) for all $g \in G$.

($\Leftarrow$) If $ghg^{-1} \in H$ for all g, h, then this is also true for g^{-1}: that is $g^{-1}hg \in H$. We now have the right side of both (a) and (b). Otherwise said, $gH = Hg$ for all $g \in G$, whence H is normal in G. ∎

Exercises 6.1. Key concepts:

Left/right cosets *normal subgroup* *(left) cosets partition group*

1. Find the cosets of the following subgroups: since the groups are abelian, left and right cosets are identical.

   (a) $4\mathbb{Z} \leq 2\mathbb{Z}$
   (b) $\langle 4 \rangle \leq \mathbb{Z}_{10}$
   (c) $\langle 6 \rangle \leq \mathbb{Z}_{30}$
   (d) $\langle 20 \rangle \leq \mathbb{Z}_{30}$

2. Find the cosets of $H = \{(0,0), (2,0), (0,2), (2,2)\} \leq \mathbb{Z}_4 \times \mathbb{Z}_4$

3. Find the left and right cosets of $\{\rho_0, \rho_1, \rho_2\} \leq D_3$. Is the subgroup normal?

4. (a) Find the left and right cosets of $H := \{e, (1\,2\,3), (1\,3\,2)\} \leq A_4$. Is the subgroup normal?
   (b) Repeat the question for the subgroup $V := \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$

5. (a) Find the left and right cosets of the subgroup $\{\rho_0, \delta_1\} \leq D_4$. Is the subgroup normal?
   (b) Repeat part (a) for the subgroup $\{\rho_0, \rho_2\}$.
   (*Hint: use cycle notation (Exercises 5.1.5.7), or look up the Cayley table*)

6. Prove Lemma 6.3: every subgroup of an abelian group is normal.

7. Suppose H is a *subset* of G, but not necessarily a subgroup.

   (a) If H has only one element, show that the sets $gH = \{gh : h \in H\}$ do partition G.
   (b) Show that the 'cosets' of $H = \{1, 3\}$ also partition $\mathbb{Z}_4$, even though H is not a subgroup.

8. Let $H = \{\sigma \in S_4 : \sigma(4) = 4\}$.

   (a) Show that H is a subgroup of S_4: we call this the *stabilizer* of 4.
   (b) Using Corollary 6.7, or otherwise, determine whether H is a normal subgroup of S_4.

9. Let H, K be subgroups of G. Define $\sim$ on G by

$$a \sim b \iff a = hbk \quad \text{for some} \quad h \in H,\ k \in K.$$

   (a) Prove that $\sim$ is an equivalence relation on G.
   (b) Describe the elements of the equivalence class of $a \in G$; this is a *double coset*.
   (c) Consider $H = \{e, (1\,2)\}$ and $K = \{e, (1\,3)\}$ as subgroups of S_3. Compute the double cosets.

6.2 Lagrange's Theorem & Indices

We've been inching up to a powerful result; with luck you've hypothesized this already!

Theorem 6.8 (Lagrange). *In a finite group, the order of a subgroup divides the order of the group.*[20] *Otherwise said*

$$H \le G \implies |H| \,\Big|\, |G|$$

Proof. Suppose $H \le G$ and fix $g \in G$. The function

$$\phi_g : H \to gH : h \mapsto gh$$

is a bijection (with inverse $\phi_g^{-1} : gh \mapsto h$). Every left coset of H therefore has the same cardinality as H. Since the left cosets partition G (Theorem 6.5), we conclude that

$$|G| = (\text{number of left cosets of } H) \cdot |H| \implies |H| \,\Big|\, |G|$$

■

We could similarly have proved this using the right coset partition. Here is an example of its power.

Corollary 6.9. *Up to isomorphism, there is a unique group of prime order p, namely $\mathbb{Z}_p$.*

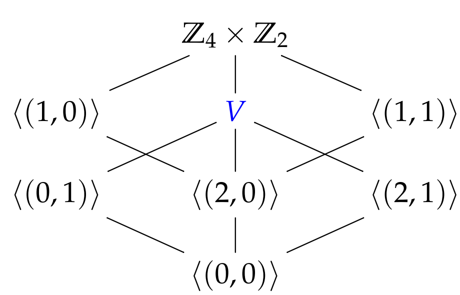
Proof. Suppose G is a group with prime order p. Since $p \ge 2$, we may choose some element $g \ne e$. The order of the cyclic subgroup $\langle g \rangle \le G$ satisfies:

- $|\langle g \rangle| \ge 2$ since $g \ne e$.
- $|\langle g \rangle| = 1$ or p by Lagrange, since p is prime.

We conclude that $|\langle g \rangle| = p \implies G = \langle g \rangle$ is cyclic and thus isomorphic to $\mathbb{Z}_p$ (Theorem 3.13). ■

Example 6.10. $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ has order 8 so its non-trivial proper subgroups can only have orders 2 or 4 and are thus isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_4$ or V. These can be identified by thinking about all possible generators; V requires three elements of order 2 which we indeed have! Here is the subgroup diagram: all proper subgroups are cyclic except $V = \{(0,0), (2,0), (0,1), (2,1)\}$.

generator	order	subgroup
$(1,0)$ or $(3,0)$	4	$\{(0,0), (1,0), (2,0), (3,0)\}$
$(1,1)$ or $(3,1)$	4	$\{(0,0), (1,1), (2,0), (3,1)\}$
$(2,0)$	2	$\{(0,0), (2,0)\}$
$(0,1)$	2	$\{(0,0), (0,1)\}$
$(2,1)$	2	$\{(0,0), (2,1)\}$
$(0,0)$	1	$\{(0,0)\}$



[20]This is sometimes misremembered as 'the order of an element divides the order of the group.' This is the special case when H is a *cyclic subgroup* of G. The even more special case when G is cyclic is Corollary 3.20: $\langle s \rangle \le \mathbb{Z}_n$ has order $\frac{n}{\gcd(s,n)}$ (certainly divides n). The converse to Lagrange is *false*: e.g. A_4 has order 12, but no subgroup of order 6 (Exercise 5.3.7).

The proof of Lagrange tells us that the *number* of left and right cosets of $H \le G$ is *identical:* both equal the quotient $\frac{|G|}{|H|}$. This motivates a new concept.

Definition 6.11. The *index* $(G : H)$ of a subgroup $H \le G$ is the cardinality of the set of (left) cosets:

$$(G : H) = |\{gH : g \in G\}|$$

The index is also the cardinality of the set of *right* cosets (Exercise 8). If G is finite, then $(G : H) = \frac{|G|}{|H|}$.

Examples 6.12. 1. If $G = \mathbb{Z}_{20}$ and $H = \langle 2\rangle$, then there are $(G : H) = \frac{20}{10} = \frac{|G|}{|H|} = 2$ cosets:

$$H = \langle 2\rangle = \{0, 2, 4, \ldots, 18\} \quad \text{and} \quad 1 + H = \{1, 3, 5, \ldots, 19\}$$

2. Recall (Example 2.21 & Exercise 2.2.10 the orthogonal and special orthogonal groups

$$\mathrm{O}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : A^T A = I\}, \qquad \mathrm{SO}_n(\mathbb{R}) = \{A \in \mathrm{O}_n(\mathbb{R}) : \det A = 1\}$$

Since every orthogonal matrix has determinant ± 1, it feels as if $\mathrm{SO}_n(\mathbb{R})$ should be 'half' of $\mathrm{O}_2(\mathbb{R})$. Since both groups are infinite (indeed uncountable), we need the index to confirm this intuition. Recall Theorem 6.5: given $A, B \in \mathrm{O}_n(\mathbb{R})$,

$$A\,\mathrm{SO}_n = B\,\mathrm{SO}_n(\mathbb{R}) \iff B^{-1}A \in \mathrm{SO}_n(\mathbb{R}) \iff \det(B^{-1}A) = 1 \iff \det B = \det A$$

We conclude that there are precisely two cosets $\big(\mathrm{O}_n(\mathbb{R}) : \mathrm{SO}_n(\mathbb{R})\big) = 2$.

Theorem 6.13. *If $K \le H \le G$ is a sequence of subgroups, then*

$$(G : K) = (G : H)(H : K)$$

If G is a finite group then the result is essentially trivial:

$$(G : K) = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = (G : H)(H : K)$$

Our proof also covers infinite groups and infinite indices. You are *strongly* encouraged to work through the following examples, which are written in the language of the proof.

Proof. Choose an element g_i from each left coset of H in G and an element h_j from each left coset of K in H. Plainly

$$(G : H) = |\{g_i\}| \qquad \text{and} \qquad (H : K) = \big|\{h_j\}\big|$$

We claim that the left cosets of K in G are precisely the sets $(g_i h_j)K$. Certainly each such is a *coset*; we show that these cosets *partition* G, whence the collection $\{(g_i h_j)K\}$ must comprise *all* left cosets.

- Every $g \in G$ lies in some left coset of H, so $\exists g_i \in G$ such that $g \in g_i H$.
  ${g_i}^{-1} g \in H$ lies in some left coset of K in H, so $\exists h_j \in H$ such that ${g_i}^{-1} g \in h_j K$.
  But then $g \in (g_i h_j)K$ so that every $g \in G$ lies in at least one set $(g_i h_j)K$.

- Suppose $y \in g_i h_j K \cap g_\alpha h_\beta K$. Since $K \leq H$ and the left cosets of H partition G, we have

$$y \in g_i H \cap g_\alpha H \implies g_\alpha = g_i$$

But then $g_i^{-1} y \in h_j K \cap h_\beta K \implies h_\beta = h_j$ similarly, since the left cosets of K in H partition H. It follows that the sets $(g_i h_j)K$ are disjoint.

Since the left cosets of K in G are given by $\{(g_i h_j)K\}$, it is immediate that

$$(G:K) = \left|\{g_i h_j\}\right| = \left|\{g_i\}\right|\left|\{h_j\}\right| = (G:H)(H:K)$$

■

Examples 6.14. 1. Recall Example 6.12.1: let $G = \mathbb{Z}_{20}$, $H = \langle 2 \rangle$ and $K = \langle 10 \rangle$. Plainly

$$K = \{0, 10\} \leq H = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\} \leq G = \{0, 1, 2, 3, \ldots, 19\}$$

so we have the required subgroup relationship. Here are the indices and cosets in each case:

- $(G:H) = 2$ with cosets H and $1 + H$. In the language of the proof, $g_0 = 0$ and $g_1 = 1$.
- $(H:K) = \frac{10}{2} = 5$ cosets, with representatives $h_0 = 0$, $h_1 = 2$, $h_2 = 4$, $h_3 = 6$, $h_4 = 8$:

$$K = \{0, 10\}, \quad 2 + K = \{2, 12\}, \quad 4 + K = \{4, 14\}, \quad 6 + K = \{6, 16\}, \quad 8 + K = \{8, 18\}$$

- $(G:K) = \frac{20}{2} = 10 = (G:H)(H:K)$: the cosets are

$$K = \{0, 10\}, \qquad 1 + K = \{1, 11\}, \qquad 2 + K = \{2, 12\}, \qquad \ldots, \qquad 9 + K = \{9, 19\}$$

In the language of the proof these cosets all have the form $(g_i + h_j) + K$.

2. Consider the sequence of subgroups $K \leq H \leq S_4$ where

$$K = \{e, (1\,2\,3), (1\,3\,2)\} \cong \mathbb{Z}_3 \quad \text{and} \quad H = \{\sigma \in S_4 : \sigma(4) = 4\} \cong S_3$$

The $(H:K) = \frac{6}{3} = 2$ left cosets of K in H are

$$K = eK = \{e, (1\,2\,3), (1\,3\,2)\} \quad \text{and} \quad (1\,2)K = \{(1\,2), (2\,3), (1\,3)\}$$

with representatives $h_0 = e$ and $h_1 = (1\,2)$. The $(S_4 : H) = \frac{24}{6} = 4$ left cosets of H in S_4 are

$$\begin{aligned}
H = eH &= \{e, (1\,2\,3), (1\,3\,2), (1\,2), (2\,3), (1\,3)\} \\
(1\,4)H &= \{(1\,4), (1\,2\,3\,4), (1\,3\,2\,4), (1\,2\,4), (1\,4)(2\,3), (1\,3\,4)\} \\
(2\,4)H &= \{(2\,4), (1\,4\,2\,3), (1\,3\,4\,2), (1\,4\,2), (2\,3\,4), (1\,3)(2\,4)\} \\
(3\,4)H &= \{(3\,4), (1\,2\,4\,3), (1\,4\,3\,2), (1\,2)(3\,4), (2\,4\,3), (1\,4\,3)\}
\end{aligned}$$

with representatives $g_0 = e$, $g_1 = (1\,4)$, $g_2 = (2\,4)$, $g_3 = (3\,4)$. The *eight* left cosets of K in S_4 are therefore

$$\begin{array}{ll}
eeK = K = \{e, (1\,2\,3), (1\,3\,2)\} & e(1\,2)K = (1\,2)K = \{(1\,2), (2\,3), (1\,3)\} \\
(1\,4)eK = (1\,4)K = \{(1\,4), (1\,2\,3\,4), (1\,3\,2\,4)\} & (1\,4)(1\,2)K = \{(1\,2\,4), (1\,4)(2\,3), (1\,3\,4)\} \\
(2\,4)eK = (2\,4)K = \{(2\,4), (1\,4\,2\,3), (1\,3\,4\,2)\} & (2\,4)(1\,2)K = \{(1\,4\,2), (2\,3\,4), (1\,3)(2\,4)\} \\
(3\,4)eK = (3\,4)K = \{(3\,4), (1\,2\,4\,3), (1\,4\,3\,2)\} & (3\,4)(1\,2)K = \{(1\,2)(3\,4), (2\,4\,3), (1\,4\,3)\}
\end{array}$$

Exercises 6.2. Key concepts:

Lagrange's Theorem *index of a subgroup*

1. Find the indices of the following subgroups:

   (a) $\langle 9\rangle \leq \mathbb{Z}_{12}$ (b) $6\mathbb{Z} \leq 2\mathbb{Z}$ (c) $(\mathbb{Q}^+, \cdot) \leq (\mathbb{Q}^\times, \cdot)$

2. Let $G = \mathbb{Z}_8$, $H = \langle 2\rangle$ and $K = \langle 4\rangle$. Write out all the cosets for the three subgroup relations $K \leq H$, $H \leq G$ and $K \leq G$, and verify the index multiplication formula.

3. Let G have order pq where p, q are both prime. Show that every proper subgroup of G is cyclic.

4. Use Lagrange's Theorem to prove that all proper subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$ are cyclic. Hence construct its subgroup diagram.

5. Find the subgroups of $\mathbb{Z}_6 \times \mathbb{Z}_2$ and draw its subgroup diagram.

   (*Hint: At least one subgroup here is* non-cyclic*!*)

6. Suppose $(G : H) = 2$. Prove that H is a normal subgroup of G.

7. Prove that $\{e\}$ and G are both normal subgroups of G: what are the cosets and the indices in each case?

   (*Remember that G could be infinite!*)

8. For each left coset gH of H in G, choose a representative g_j. Prove that the function

   $$\Phi : g_j H \mapsto H g_j^{-1}$$

   defines an injective function from the set of left cosets to the set of right cosets.

   With the reverse argument this shows that the sets of left and right cosets have the same cardinality

9. Let $G = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

   (a) Prove that G is a group under addition.

   (b) Prove that $H = \{3m + 2n\sqrt{2} : m, n \in \mathbb{Z}\}$ is a subgroup of index six in G.
   (*Hint: what does it mean for $a + b\sqrt{2}$ and $c + d\sqrt{2}$ to lie in the same coset of H?*)

10. The sets $\mathbb{Q}$ and $\mathbb{Z}$ are both groups under addition. Show that there is precisely one coset of $\mathbb{Z}$ in $\mathbb{Q}$ for each rational number in the interval $[0, 1)$. Hence conclude that $(\mathbb{Q} : \mathbb{Z}) = \aleph_0$ is countably infinite.

6.3 Factor Groups

Given a subgroup $H \le G$, we ask whether the *set of left cosets* $\{gH : g \in G\}$ can be viewed as a group *in a natural way*. By this, we mean that the group structure on should be *inherited* from that of G. To see how this works (or doesn't!), recall Examples 6.1.

Examples (6.4.1 cont). 1. The set of (left) cosets for $H = \langle 4 \rangle = \{0,4,8\} \le \mathbb{Z}_{12}$ is

$$\{H,\, 1+H,\, 2+H,\, 3+H\} = \Big\{\{0,4,8\},\{1,5,9\},\{2,6,10\},\{3,7,11\}\Big\}$$

It feels like we have the cyclic group $\mathbb{Z}_4$ in disguise! To see this we need a binary operation: the natural approach is to use the addition we already have in $\mathbb{Z}_{12}$ and define addition of cosets via

$$(a+H) \oplus (b+H) := (a+b)+H$$

The process for computing $(a+H) \oplus (b+H)$ contains a potential snag:

(a) *Choose representatives*: Make a choice of elements a and b in the respective cosets.
(b) *Add within the original group*: Compute $a+b \in \mathbb{Z}_{12}$.
(c) *Take the coset*: Return the left coset $(a+b)+H$.

If $\oplus$ is to make sense, the outcome must be *independent of the choices* made in step (a). In this case there is no problem, as you can tediously check for yourself: for example, to verify

$$(2+H) \oplus (3+H) = 1+H$$

there are *nine* possibilities, of which one is

$$6 +_{12} 11 = 17 = 5 \in 1+H$$

Rather than verify these independently, we proceed in general. If $x \in a+H$ and $y \in b+H$, then $x-a$ and $y-b \in H$, whence

$$(x-a)+(y-b) = (x+y)-(a+b) \in H \implies (x+y)+H = (a+b)+H$$

The operation is well-defined and we'll shortly see that the set of left cosets forms a group under $\oplus$. Indeed $\phi(x) = x+H$ defines an isomorphism of $\mathbb{Z}_4$ with this *factor group.*

2. Unfortunately, this sort of behavior isn't universal. Let us repeat the process with the subgroup $H = \{e, \mu_1\} \le D_3$, whose left cosets are

$$H = \mu_1 H = \{e,\mu_1\}, \quad \rho_1 H = \mu_3 H = \{\rho_1, \mu_3\}, \quad \rho_2 H = \mu_2 H = \{\rho_2, \mu_2\}$$

This time, if we attempt to define the 'natural' operation on the set $\{\sigma H\}$ of left cosets via

$$aH \otimes bH := (ab)H$$

then the problem is real. There are *four choices* for how to compute $\rho_1 H \otimes \rho_1 H$, of which two suffice for a contradiction:

$$\rho_1\rho_1 H = \rho_2 H \quad \text{and} \quad \mu_3\mu_3 H = H$$

The freedom of choice (part (a)) in the definition of $\otimes$ leads to different outcomes, whence $\otimes$ is *not well-defined*, and the set of left cosets does not form a group in a natural way.

Well-definition of the Factor Group Structure

As the examples show, some subgroups $H \leq G$ behave better than others when trying to view the set of left cosets as a group. But which subgroups? To answer this, we repeat some of our discussion in the abstract.

Let H be a subgroup of G and define the natural operation on the set of left cosets:

$$aH \cdot bH := (ab)H$$

This is well-defined if and only if

$$\forall a, b \in G,\ \forall x \in aH,\ y \in bH, \quad \text{we have} \quad (ab)H = (xy)H$$

Let us trace through what this means for the subgroup H, using the fact that

$$x \in aH \iff \exists h \in H \text{ such that } x = ah$$

The natural operation is well-defined if and only if

$$\begin{aligned} &\forall a, b \in G,\ h, h_1 \in H,\ (ab)H = (ahbh_1)H = (ahb)H \\ \iff &\forall a, b \in G,\ h \in H,\ (ab)^{-1}(ahb) \in H && \text{(Theorem 6.5)} \\ \iff &\forall b \in G,\ h \in H,\ b^{-1}hb \in H \\ \iff &H \lhd G && \text{(Corollary 6.7)} \end{aligned}$$

We have proved the critical part of an amazing result!

Theorem 6.15. *Suppose $H \leq G$. The set of left cosets forms a group under the natural operation*

$$aH \cdot bH := (ab)H$$

if and only if H is a normal subgroup of G.

Definition 6.16. If $H \lhd G$, then the set of (left) cosets is a *factor group*, written ${}^{G}/_{H}$ ('G mod H').

Since the group structure on ${}^{G}/_{H}$ arises naturally from that on G, we typically use the *same notation* for the operation. The notation meshes with the index: if G is finite, then $\left|{}^{G}/_{H}\right| = (G : H) = \frac{|G|}{|H|}$.

Proof. The above discussion shows that the natural operation on ${}^{G}/_{H}$ is well-defined if and only if H is normal in G. It remains only to check that ${}^{G}/_{H}$ is a group in such cases.

Closure: $aH \cdot bH = (ab)H$ is a coset, whence $\left({}^{G}/_{H}, \cdot\right)$ is closed.

Associativity: $aH \cdot (bH \cdot cH) = aH \cdot (bc)H = a(bc)H$. Similarly $(aH \cdot bH) \cdot cH = (ab)cH$. By the associativity of G these cosets are identical.

Identity: $eH \cdot aH = (ea)H = aH = (ae)H = aH \cdot eH$ therefore the *identity coset* $eH = H$ is the identity.

Inverse: $a^{-1}H \cdot aH = (a^{-1}a)H = eH = H$, etc., therefore $(aH)^{-1} = a^{-1}H$. ∎

Factor Groups of $\mathbb{Z}$: modular arithmetic done right!

For each positive integer n, the integer multiples $n\mathbb{Z} = \langle n \rangle$ form a normal subgroup of $\mathbb{Z}$. The coset of $n\mathbb{Z}$ containing $x \in \mathbb{Z}$ is therefore

$$x + n\mathbb{Z} = \{x + kn : k \in \mathbb{Z}\} = \{y \in \mathbb{Z} : y \equiv x \pmod{n}\}$$

This is precisely what we are used to calling 'x' in $\mathbb{Z}_n$! Indeed this is the formal definition, superseding Definition 3.4 and trivially proving Theorem 3.5.

Definition 6.17. Let $n \in \mathbb{N}$. The group $\mathbb{Z}_n$ is the *factor group* $\mathbb{Z}/_{n\mathbb{Z}}$

Since remainders are so familiar, we typically drop $n\mathbb{Z}$ when calculating, thus

$$4 + 5 = 2 \in \mathbb{Z}_7 \quad \text{means} \quad (4 + 7\mathbb{Z}) + (5 + 7\mathbb{Z}) = 2 + 7\mathbb{Z} \in \mathbb{Z}/_{7\mathbb{Z}}$$

Factor Groups of Finite Cyclic Groups

Our first example in this section showed that $\mathbb{Z}_{12}/_{\langle 4 \rangle} \cong \mathbb{Z}_4$. Here is another.

Example 6.18. $\langle 5 \rangle = \{0, 5, 10, 15\} \leq \mathbb{Z}_{20}$ has factor group

$$\mathbb{Z}_{20}/_{\langle 5 \rangle} = \{0 + \langle 5 \rangle, 1 + \langle 5 \rangle, 2 + \langle 5 \rangle, 3 + \langle 5 \rangle, 4 + \langle 5 \rangle\}$$

This is isomorphic to $\mathbb{Z}_5$ via the isomorphism

$$\psi : \mathbb{Z}_5 \to \mathbb{Z}_{20}/_{\langle 5 \rangle} : x \mapsto x + \langle 5 \rangle$$

Theorem 6.19. *If $d \mid n$, then $\mathbb{Z}_n/_{\langle d \rangle} \cong \mathbb{Z}_d$.*

If s is not a divisor of n, recall that $\langle s \rangle = \langle d \rangle$ where $d = \gcd(s, n)$, whence $\mathbb{Z}_n/_{\langle s \rangle} \cong \mathbb{Z}_{\gcd(s,n)}$.

Proof. Define $\psi : \mathbb{Z}_d \to \mathbb{Z}_n/_{\langle d \rangle} : x \mapsto x + \langle d \rangle$: our goal is to see that this is an isomorphism.

Well-definition/injectivity:[21] The former is required since the domain is a set of *equivalence classes*!

$$x = y \in \mathbb{Z}_d \iff x - y \in \langle d \rangle \iff x + \langle d \rangle = y + \langle d \rangle \iff \psi(x) = \psi(y)$$

Surjectivity: Any coset $x + \langle d \rangle = \psi(x) \in \operatorname{Im}(\psi)$.

Homomorphism: For any $x, y \in \mathbb{Z}_d$,

$$\psi(x + y) = (x + y) + \langle d \rangle = \big(x + \langle d \rangle\big) + \big(y + \langle d \rangle\big) = \psi(x) + \psi(y)$$

∎

[21] That these arguments are converses is typical: for a given function $\mu : A \to B$,

- Well-definition means: $a = b \implies \mu(a) = \mu(b)$
- Injectivity means: $\mu(a) = \mu(b) \implies a = b$

Finite Abelian Examples

If G is a finite abelian group, then any subgroup H is normal and ${}^{G}/_{H}$ is also a finite abelian group (exercise). By the Fundamental Theorem (4.9) there exist positive integers $m_1, \ldots, m_k$ for which

$$ {}^{G}/_{H} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k} \quad \text{and} \quad m_1 \cdots m_k = (G : H) = \frac{|G|}{|H|} $$

Our goal in these examples is to *identify* ${}^{G}/_{H}$ as a direct product by finding suitable integers m_k.

Examples 6.20. For $G = \mathbb{Z}_4 \times \mathbb{Z}_8$ and three subgroups H, we identify the factor group ${}^{G}/_{H}$.

1. If $H = \langle (0,1) \rangle = \{(0,0),(0,1),(0,2),\ldots,(0,7)\}$, then the index of H in G is $(G : H) = \frac{4 \cdot 8}{8} = 4$. The factor group is abelian with order four and thus isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

   Here are two strategies for deciding which.

   (a) Identify the cosets:

   $$ (x,y) + H = (v,w) + H \iff (x,y) - (v,w) = (x-v, y-w) \in H \iff x = v $$

   Each coset contains a unique element $(x,0)$ where $x \in \mathbb{Z}_4$, whence,

   $$ {}^{G}/_{H} = \Big\{ H,\ (1,0)+H,\ (2,0)+H,\ (3,0)+H \Big\} $$

   It can be checked that this is isomorphic to $\mathbb{Z}_4$ via $\psi : \mathbb{Z}_4 \to {}^{G}/_{H} : x \mapsto (x,0) + H$.

   (b) Observe that there exists an element in ${}^{G}/_{H}$ with order 4. If $k \in \mathbb{N}$, then

   $$ k\big((1,0)+H\big) = (k,0) + H = H \iff (k,0) \in H \iff 4 \mid k $$

   This identifies ${}^{G}/_{H} \cong \mathbb{Z}_4$ by elimination: every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order *at most* 2.

2. $H = \langle (0,2) \rangle = \{(0,0),(0,2),(0,4),(0,6)\}$ has order 4 with index $(G : H) = \frac{4 \cdot 8}{4} = 8$. The factor group is abelian with order 8 and thus isomorphic to one of $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

   We again follow our strategies:

   (a) Identify the cosets:

   $$ (x,y) + H = (v,w) + H \iff (x-v, y-w) \in H \iff \begin{cases} x = v, \text{and} \\ y - w = 2k \text{ is even} \end{cases} $$

   from which the distinct cosets may be written

   $$ {}^{G}/_{H} = \Big\{ H,\ (1,0)+H,\ (2,0)+H,\ \ldots\ (3,1)+H \Big\} = \Big\{ (x,y) + H : x \in \mathbb{Z}_4, y \in \mathbb{Z}_2 \Big\} $$

   We have an isomorphism $\psi : \mathbb{Z}_4 \times \mathbb{Z}_2 \to {}^{G}/_{H} : (x,y) \mapsto (x,y) + H$.

   (b) Alternatively, consider orders of elements:

   - ${}^{G}/_{H}$ contains an element $(1,0) + H$ of order 4.
   - All elements of ${}^{G}/_{H}$ have order dividing 4:

   $$ 4\big((x,y)+H\big) = (4x,4y) + H = (0,4y) + H = 2y\big((0,2)+H\big) = H $$

   By elimination, ${}^{G}/_{H} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ ($\mathbb{Z}_8$ has an element of order 8, while elements of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ have maximum order 2).

3. Consider $H = \langle(2,4)\rangle = \{(0,0),(2,4)\}$. The previous examples may have lulled you into a false sense of security: $G/_{H}$ is *not*

$$\mathbb{Z}_4/_{\langle 2\rangle} \times \mathbb{Z}_8/_{\langle 4\rangle} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

The fact that there are $(G:H) = \frac{4\cdot 8}{2} = 16$ cosets immediately rules out this naïve possibility!

The Fundamental Theorem gives *five* non-isomorphic options for the factor group:

$$\mathbb{Z}_{16}, \ \ \mathbb{Z}_2 \times \mathbb{Z}_8, \ \ \mathbb{Z}_4 \times \mathbb{Z}_4, \ \ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \ \ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

We again follow our strategies:

(a) Identify the cosets. This is a little trickier than before.

- If $x = 2n$ is even, then

$$(x,y) + H = (2n,y) + H = n(2,4) + (0, y-4n) + H = (0, y-4n) + H$$

- If $x = 2n+1$ is odd, then

$$(x,y) + H = (2n+1,y) + H = n(2,4) + (1, y-4n) + H = (1, y-4n) + H$$

There is precisely one representative of each coset whose first entry is either 0 or 1, whence the sixteen elements

$$(0,0),\ (0,1),\ \ldots,\ (0,7),\ (1,0),\ \ldots,\ (1,7)$$

lie in distinct cosets of H. It seems reasonable to claim that the factor group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_8$. Indeed

$$\psi : \mathbb{Z}_2 \times \mathbb{Z}_8 \to G/_{H} \to: (x,y) \mapsto (x, y-2x) + H$$

is an explicit isomorphism. We leave it as an exercise to verify this. It requires some creativity to invent such a function from nothing, particularly at the moment!

(b) The coset $(0,1) + H$ has order 8 in $G/_{H}$, since

$$k\big((0,1)+H\big) = (0,k) + H = H \iff 8 \mid k$$

which reduces our options to $\mathbb{Z}_{16}$ and $\mathbb{Z}_2 \times \mathbb{Z}_8$. Moreover, any coset has order dividing 8:

$$8\Big((x,y)+H\Big) = (8x, 8y) + H = (0,0) + H$$

This rules out $\mathbb{Z}_{16}$, leaving $\mathbb{Z}_2 \times \mathbb{Z}_8$ as the only possibility.

Strategy (b) might seem easier right now, but it has some drawbacks; for instance, it cannot distinguish between groups such as $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$: both groups contain an element of order 4, and the maximum order of an element is also 4.

Other Examples

There are many other examples of factor groups, with varied strategies required for their identification. Here are just a few, and we'll see more in later chapters.

Examples 6.21. 1. $\langle 2\pi \rangle = 2\pi\mathbb{Z} = \{2\pi n : n \in \mathbb{Z}\}$ is a subgroup of the abelian group $(\mathbb{R}, +)$.

In any given coset $x + 2\pi\mathbb{Z}$, there is a unique x such that $0 \leq x < 2\pi$ (this is like taking the remainder of x modulo 2π!). It follows that

$$\mathbb{R}/_{2\pi\mathbb{Z}} = \{x + 2\pi\mathbb{Z} : x \in [0, 2\pi)\}$$

Moreover, the function

$$\mu : \mathbb{R}/_{2\pi\mathbb{Z}} \to S^1 : x + 2\pi\mathbb{Z} \mapsto e^{ix}$$

is an isomorphism of groups. The factor group construction therefore corresponds to wrapping the real line infinitely many times around a circle of circumference 2π.

2. Exercise 6.1.4, tells us that the Klein four-group

$$V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

is a normal subgroup of the alternating group A_4. The factor group has order $(A_4 : V) = \frac{12}{4} = 3$ and so $A_4/_V \cong \mathbb{Z}_3$: can you find an explicit isomorphism?

It's a lot harder to prove, but we'll see later that $S_4/_V \cong S_3$.

3. Consider $H = \langle (2, 1) \rangle \leq \mathbb{Z} \times \mathbb{Z}_4 = G$. Since G and H are infinite, we cannot simply apply the index formula to count cosets. Instead we use the 2 in the subgroup H to find a simple representative of each coset.

$$(x, y) + H = \begin{cases} (2n, y) + H = (0, y - n) + H & \text{if } x = 2n \text{ is even} \\ (2n + 1, y) + H = (1, y - n) + H & \text{if } x = 2n + 1 \text{ is odd} \end{cases}$$

There is a *unique representative* in each coset either of the form $(0, z)$ or $(1, z)$, where $z \in \mathbb{Z}_4$. We conclude that there are $2 \cdot 4 = 8$ cosets. Since $G/_H$ is abelian (Exercise 6), it must be isomorphic to one of $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. To identify which, compute

$$4\big((x, y) + H\big) = (4x, 4y) + H = (0, -2x) + H = H \iff 2 \mid x$$

We conclude that $(1, 0) + H$ has order 8, whence $G/_H \cong \mathbb{Z}_8$.

4. Let $H = \langle (1, 2) \rangle \leq \mathbb{Z} \times \mathbb{Z} = G$. We play a similar trick as above

$$(x, y) + H = (0, y - 2x) + H$$

Since the choice of y is free, we see that there is a unique representative in each coset of the form $(0, z)$. We conclude that $G/_H \cong \mathbb{Z}$. In fact it can be checked that $\psi\big((x, y) + H\big) = y - 2x$ defines an isomorphism.

Exercises 6.3. Key concepts:

Factor group *well-definition* $\iff H \triangleleft G$ $\mathbb{Z}_n := {}^{\mathbb{Z}}/_{n\mathbb{Z}}$ *identifying* ${}^{G}/_{H}$

1. List the cosets of the subgroup $H = \langle 3 \rangle$ in $G = \mathbb{Z}_{15}$. Verify directly that the function
$$\psi : \mathbb{Z}_3 \mapsto {}^{G}/_{H} : x \mapsto x + H$$
is a well-defined homomorphism (mimic the proof of Theorem 6.19!).

2. Identify the factor group ${}^{\mathbb{Z}_4 \times \mathbb{Z}_4}/_{H}$, where $H = \{(0,0),(0,2),(2,0),(2,2)\}$ (Exercise 6.1.2).

3. (a) Identify the factor group ${}^{G}/_{H}$ where $H = \langle (2,4) \rangle \leq G = \mathbb{Z}_4 \times \mathbb{Z}_6$.
   (b) Repeat with the subgroup $H = \langle 2 \rangle \times \langle 4 \rangle$ (*this is a trick question!*)

4. (a) Let $G = \mathbb{Z}_9 \times \mathbb{Z}_9$ and $H = \langle (3,6) \rangle$. Identify ${}^{G}/_{H}$ by showing that every element of the factor group has order at most 9 and that it contains an element of order 9.
   (b) Repeat with $H = \langle 3 \rangle \times \langle 6 \rangle$ (*this isn't a trick question!*)

5. Let G be any group. To what groups are ${}^{G}/_{\{e\}}$ and ${}^{G}/_{G}$ isomorphic?

6. (a) If G is abelian and $H \leq G$, prove that ${}^{G}/_{H}$ is abelian.
   (b) If ${}^{G}/_{H}$ is abelian, can we conclude that G and/or H is abelian? Explain.

7. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_8$. Prove that each function in Examples 6.20 is a well-defined homomorphism.
   (a) $H = \langle (0,1) \rangle$, $\psi : \mathbb{Z}_4 \to {}^{G}/_{H} : x \mapsto (x,0) + H$
   (b) $H = \langle (0,2) \rangle$, $\psi : \mathbb{Z}_4 \times \mathbb{Z}_2 \to {}^{G}/_{H} : (x,y) \mapsto (x,y) + H$
   (c) $H = \langle (2,4) \rangle$, $\psi : \mathbb{Z}_2 \times \mathbb{Z}_8 \to {}^{G}/_{H} : (x,y) \mapsto (x, y-2x) + H$

   (*Bijectivity follows from the description of the cosets, though proving injectivity might be instructive.*)

8. Recall Exercise 6.2.9. The factor group ${}^{G}/_{H}$ is abelian and of order 6, whence it is cyclic. Prove this explicitly by finding a generator.

9. (a) Let G be a cyclic group with subgroup H. Prove that ${}^{G}/_{H}$ is cyclic.
   (b) If ${}^{G}/_{H}$ is cyclic, does it follow that G is cyclic? Prove or disprove.

10. In Example 6.21.2 we saw that $\mathbb{Z}_3 \cong {}^{A_4}/_{V}$. Find an explicit isomorphism.

11. Exercise 6.1.5 showed that $\{\rho_0, \rho_2\}$ is a normal subgroup of D_4. To what well-known group is the factor group ${}^{D_4}/_{\{\rho_0,\rho_2\}}$ isomorphic? Prove your assertion.

12. Let $H = \langle (2,3) \rangle \leq G = \mathbb{Z}_5 \times \mathbb{Z}$. Prove that ${}^{G}/_{H} \cong \mathbb{Z}_{15}$.

13. Verify the claim in Example 6.21.4 that $\psi\big((x,y) + H\big) = y - 2x$ is an isomorphism.

14. (Hard!) Let $G = \mathbb{Z}_{10} \times \mathbb{Z}_6 \times \mathbb{Z}$ and $H = \langle (4,2,3) \rangle$. Identify the factor group ${}^{G}/_{H}$ as a direct product $\mathbb{Z}_m \times \mathbb{Z}_n$.
    (*Hint: use the division algorithm $z = 3q + r$ to show that there is exactly one representative of each coset $(x,y,z) + H$ where z is either 0, 1 or 2.*)

7 Homomorphisms and the First Isomorphism Theorem

In this chapter we further discuss homomorphisms. Of particular importance is the relationship between normal subgroups, homomorphisms and factor groups.
Unless otherwise stated, in this chapter all homomorphisms are between *groups*.

7.1 Kernels and Images

Definition 7.1. Let $\phi : G \to L$ be a homomorphism. The *kernel* and *image* (or *range*) of ϕ are the sets

$$\ker\phi = \{g \in G : \phi(g) = e_L\} \qquad \operatorname{Im}\phi = \{\phi(g) : g \in G\}$$

The image is sometimes denoted $\phi(G)$. Note that $\ker\phi \subseteq G$ while $\operatorname{Im}\phi \subseteq L$.

Examples 7.2. 1. $\phi(x) = 2x \pmod 4$ defines a homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_4$, with

$$\ker\phi = \{x \in \mathbb{Z} : 2x \equiv 0 \pmod 4\} = 2\mathbb{Z}, \quad \operatorname{Im}\phi = \{0, 2\}$$

2. The kernel should feel familiar from linear algebra: if $\mathrm{T} : V \to W$ is a linear map between vector spaces, then the kernel is simply the *nullspace*

$$\ker\mathrm{T} = \{\mathbf{v} \in V : \mathrm{T}(\mathbf{v}) = \mathbf{0}\}$$

Moreover, if $\mathrm{T} = \mathrm{L}_A : M_n(\mathbb{R}) \to M_m(\mathbb{R})$ is left-multiplication by a matrix A, then $\operatorname{Im}\mathrm{T}$ is the *column space* of A.

Lemma 7.3. *Let $\phi : G \to L$ be a homomorphism. Then,*

1. $\phi(e_G) = e_L$ *(ϕ maps identity to identity)*
2. $\forall g \in G,\ \big(\phi(g)\big)^{-1} = \phi(g^{-1})$ *(ϕ maps inverses to inverses)*
3. $\ker\phi \lhd G$ *($\ker\phi$ is a normal subgroup of G)*
4. $\operatorname{Im}\phi \leq L$ *($\operatorname{Im}\phi$ is a subgroup of L)*

Proof. 1 & 2 were in Exercise 2.3.6 and we leave 4 as an exercise. We prove 3 explicitly.

3. Suppose $k_1, k_2 \in \ker\phi$. Then

$$\phi(k_1k_2) = \phi(k_1)\phi(k_2) = e_L \implies k_1k_2 \in \ker\phi$$
$$\phi(k_1^{-1}) = \big(\phi(k_1)\big)^{-1} = e_L \implies k_1^{-1} \in \ker\phi$$

It follows that $\ker\phi$ is a subgroup of G.
To see that $\ker\phi$ is normal, recall Corollary 6.7: if $g \in G$ and $k \in \ker\phi$, then

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_L \implies gkg^{-1} \in \ker\phi$$

■

Examples 7.4. 1. For the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_4 : x \mapsto 2x$, we see that $\ker\phi = 2\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$, and $\operatorname{Im}\phi = \{0, 2\} = \langle 2 \rangle$ a subgroup of $\mathbb{Z}_4$.

2. The nullspace of a linear map $\mathrm{T} : V \to W$ is indeed a *subspace* and thus a subgroup $\ker \mathrm{T} \leq V$: since V is abelian, this is a normal subgroup. Moreover, $\operatorname{Im}\mathrm{T}$ is also a subspace/group of W.

3. $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism, whence we obtain a normal subgroup

$$\ker\det = \mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) : \det A = 1\} \triangleleft \mathrm{GL}_n(\mathbb{R})$$

4. $\phi : \mathbb{Z} \to \mathbb{Z}_{20} : x \mapsto 4x \pmod{20}$ is a homomorphism, as may be checked:

$$\phi(x+y) = 4(x+y) = 4x + 4y = \phi(x) + \phi(y) \in \mathbb{Z}_{20}$$

Its kernel and image are $\ker\phi = 5\mathbb{Z} \leq \mathbb{Z}$ and $\operatorname{Im}\phi = \langle 4 \rangle = \{0, 4, 8, 12, 16\} \leq \mathbb{Z}_{20}$

Since every kernel is a normal subgroup, it is worth identifying the distinct cosets with a view to describing the factor group ${}^{G}/_{\ker\phi}$.

Lemma 7.5. *Let $\phi : G \to L$ be a homomorphism. Then*

$$g_1 \ker\phi = g_2 \ker\phi \iff \phi(g_1) = \phi(g_2)$$

There is precisely one coset of $\ker\phi$ for each element of $\operatorname{Im}\phi$; otherwise said $(G : \ker\phi) = |\operatorname{Im}\phi|$.

Proof. For all $g_1, g_2 \in G$, we have

$$\begin{aligned} g_1 \ker\phi = g_2 \ker\phi &\iff g_2^{-1} g_1 \in \ker\phi && \text{(Theorem 6.5)} \\ &\iff \phi(g_2^{-1} g_1) = e_L && \text{(Definition 7.1)} \\ &\iff \phi(g_2)^{-1}\phi(g_1) = e_L && \text{(Lemma 7.3)} \\ &\iff \phi(g_1) = \phi(g_2) \end{aligned}$$

∎

We'll extend this idea shortly; for the moment we use it to aid in finding homomorphisms.

Theorem 7.6. *Let $\phi : G \to L$ be a homomorphism. If G (or L) is finite, then $\operatorname{Im}\phi$ is a finite group whose order divides that of G (or L). Otherwise said:*

$$|G| < \infty \implies |\operatorname{Im}\phi| \,\Big|\, |G| \quad \textit{and} \quad |L| < \infty \implies |\operatorname{Im}\phi| \,\Big|\, |L|$$

Proof. If G is a finite group, then $\ker\phi \leq G$ is finite. Now apply Lemma 7.5:

$$|\operatorname{Im}\phi| = (G : \ker\phi) = \frac{|G|}{\ker\phi}$$

is a divisor of $|G|$. The second case $|\operatorname{Im}\phi| \,\Big|\, |L|$ is Lagrange's Theorem (6.8).

∎

Examples 7.7. 1. How many distinct homomorphisms are there $\phi : \mathbb{Z}_{17} \to \mathbb{Z}_{13}$?

If ϕ is such a homomorphism, the Theorem says that $|\operatorname{Im}\phi|$ divides both 17 and 13. The only such positive integer is 1. Since $\operatorname{Im}\phi$ must contain the identity, we conclude that there is only one homomorphism!

$$\forall x \in \mathbb{Z}_{17},\ \phi(x) = 0$$

More generally, if $\gcd(|G|, |L|) = 1$, then the only homomorphism $\phi : G \to L$ is the trivial function $\phi : g \mapsto e_L$.

2. Describe all homomorphisms $\phi : \mathbb{Z}_4 \to S_3$.

Since the domain $\mathbb{Z}_4$ is cyclic, we need only describe what happens to a generator (e.g. 1) to obtain the entire homomorphism $\phi(x) = \big(\phi(1)\big)^x$. There are at most *six* homomorphisms; one for each possible element $\phi(1) \in S_3$. Not all of these cases are however possible.

The Theorem says that $|\operatorname{Im}\phi| = 1$ or 2; the only common divisors of $4 = |\mathbb{Z}_4|$ and $6 = |S_3|$.

If $\operatorname{Im}\phi$ has one element, we obtain the trivial homomorphism $\phi_(x) = e$, $\forall x \in \mathbb{Z}_4$.

If $|\operatorname{Im}\phi| = 2$, then $\operatorname{Im}\phi$ is a subgroup of order 2 of which S_3 contains exactly three: $\{e, (2\,3)\}$, $\{e, (1\,3)\}$, $\{e, (1\,2)\}$. We therefore have three further homomorphisms

$$\phi_1(x) = (2\,3)^x, \quad \phi_2(x) = (1\,3)^x, \quad \phi_3(x) = (1\,2)^x$$

for a grand total of four distinct homomorphisms.

We now consider the general question of homomorphisms between finite cyclic groups $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$. Two facts make this relatively simple:

1. It is enough to define $\phi(1)$, for then $\phi(x) = \phi(1) + \cdots + \phi(1) = \phi(1) \cdot x$.
2. $|\operatorname{Im}\phi|$ must divide $d := \gcd(m, n)$. Since $\mathbb{Z}_n$ has exactly one subgroup of each order dividing n (Corollary 3.20), $\operatorname{Im}\phi$ must be a subgroup of the unique subgroup of $\mathbb{Z}_n$ of order d:

$$\operatorname{Im}\phi \le \left\langle \frac{n}{d} \right\rangle = \left\{ 0, \frac{n}{d}, \frac{2n}{d}, \ldots, \frac{(d-1)n}{d} \right\}$$

We need only try letting $\phi(1)$ be each element of this group in turn...

Corollary 7.8. *There are $d = \gcd(m, n)$ distinct homomorphisms $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$, defined by*

$$\phi_k(x) = \frac{kn}{d} x \quad \text{where} \quad k = 0, \ldots, d-1$$

Proof. Following the above, it remains only to check that each ϕ_k is a well-defined function. For this, note first that $x = y \in \mathbb{Z}_m \iff y = x + \lambda m$ for some $m \in \mathbb{Z}$, from which

$$\phi_k(y) = \phi_k(x + \lambda m) = \frac{kn}{d}(x + \lambda m) = \frac{kn}{d}x + \lambda k \frac{m}{d} n = \frac{kn}{d}x = \phi_k(x) \qquad (\text{in } \mathbb{Z}_n)$$

where we used the fact that $\frac{m}{d}$ is an *integer*. ∎

Example 7.9. We describe all homomorphisms $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{20}$.
Since $\gcd(12, 20) = 4$, we see that $\operatorname{Im}\phi \le \langle 5 \rangle = \{0, 5, 10, 15\} \le \mathbb{Z}_{20}$. There are four choices:

$$\phi_0(x) = 0, \qquad \phi_1(x) = 5x, \qquad \phi_2(x) = 10x, \qquad \phi_3(x) = 15x \pmod{20}$$

Reversing the argument, we see that there are also four distinct homomorphisms $\psi : \mathbb{Z}_{20} \to \mathbb{Z}_{12}$:

$$\psi_0(x) = 0, \qquad \psi_1(x) = 3x, \qquad \psi_2(x) = 6x, \qquad \psi_3(x) = 9x \pmod{12}$$

Exercises 7.1. Key concepts:

Image *kernels are normal subgroups* $(G : \ker\phi) = |\operatorname{Im}\phi|$ $|\operatorname{Im}\phi| \,\Big|\, \gcd(|G|, |L|)$

1. Check that you have a homomorphism (use Corollary 7.8) and compute its kernel and image.
   (a) $\phi : \mathbb{Z}_8 \to \mathbb{Z}_{14}$ defined by $\phi(x) = 7x \pmod{14}$.
   (b) $\phi : \mathbb{Z}_{36} \to \mathbb{Z}_{20}$ defined by $\phi(x) = 5x \pmod{20}$.
2. Describe all homomorphisms between the groups:
   (a) $\phi : \mathbb{Z}_{15} \to \mathbb{Z}_{80}$
   (b) $\phi : \mathbb{Z} \to \mathbb{Z}_3$
   (c) $\phi : \mathbb{Z}_6 \to D_4$
   (d) $\phi : \mathbb{Z}_{15} \to A_4$
3. Find the kernel and image of each homomorphism.
   (a) The *trace* of a matrix: $\operatorname{tr} : M_2(\mathbb{R}) \to \mathbb{R}$ defined by $\operatorname{tr}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a + d = a + d$
   (b) $T : \mathbb{R}^3 \to \mathbb{R}^4 : \mathbf{x} \mapsto \begin{pmatrix} 1 & 1 & -1 \\ 0 & 3 & -1 \\ 1 & 4 & -2 \\ 2 & 5 & -3 \end{pmatrix}$ (*Hint: remember row operations...*)
4. Explain why the map ϕ is a homomorphism and find $\ker\phi$:
$$\phi : S_n \to \big(\{1, -1\}, \cdot\big) : \sigma \mapsto \begin{cases} 1 & \text{if } \sigma \text{ even} \\ -1 & \text{if } \sigma \text{ odd} \end{cases}$$
5. (a) Prove Part 4 of Lemma 7.3: if $\phi : G \to L$ is a homomorphism, then $\operatorname{Im}\phi \le L$.
   (b) If $H \le G$ and $\phi : G \to L$ a homomorphism, prove that $\phi(H) := \{\phi(h) : h \in H\} \le \operatorname{Im}\phi$.
   (c) Give an example to show that $\operatorname{Im}\phi$ need not be a normal subgroup of L.
6. Prove that the number of distinct *isomorphisms* $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ equals the cardinality of the group of units in $\mathbb{Z}_n$ (see Exercise 3.2.10))
$$\left|\mathbb{Z}_n^\times\right| = |\{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}|$$
7. Prove that $\phi : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n$ is a well-defined homomorphism if and only if there exist integers a, b, c, d for which
$$\phi(x, y) = \big(ax + by, cx + dy\big), \quad m \mid bn \quad \text{and} \quad n \mid cm$$
   (*Hint: let* $(a, c) = \phi(1, 0)$*, etc.*)
8. Find all homomorphisms $\phi : \mathbb{Z}_2 \times \mathbb{Z}_7 \to \mathbb{Z}_2 \times \mathbb{Z}_5$. How do you know that there are no more?
9. Consider $\phi : D_4 \to D_4 : \sigma \mapsto \sigma^2$. Show that ϕ is *not* a homomorphism.

7.2 The First Isomorphism Theorem

We've seen that all kernels of group homomorphisms are normal subgroups. In fact *all* normal subgroups are the kernel of some homomorphism.

Theorem 7.10 (Canonical Homomorphism). *Let G be a group and $H \triangleleft G$. Then the function*

$$\gamma : G \to {}^{G}\!/_{H} \quad \textit{defined by} \quad \gamma(g) = gH$$

is a homomorphism with $\ker \gamma = H$.

Proof. Since H is normal, ${}^{G}\!/_{H}$ is a group. By the definition of multiplication in ${}^{G}\!/_{H}$,

$$\gamma(g_1)\gamma(g_2) = g_1H \cdot g_2H = (g_1g_2)H = \gamma(g_1g_2)$$

whence γ is a group homomorphism. Moreover, the identity in the factor group is H, whence

$$\ker \gamma = \{g \in G : \gamma(g) = H\} = \{g \in G : gH = H\} = H$$

■

This might feel a little sneaky and unsatisfying; we'd perhaps have preferred a homomorphism that doesn't have a factor group as its image! However, the following companion result says that, among homomorphisms with the same kernel, γ is unavoidable.

Theorem 7.11 (1st Isomorphism Thm). *Let $\phi : G \to L$ be a homomorphism with kernel H. Then*

$$\mu : {}^{G}\!/_{H} \to \operatorname{Im}\phi \quad \textit{defined by} \quad \mu(gH) = \phi(g)$$

is an isomorphism. Otherwise said, ${}^{G}\!/_{\ker\phi} \cong \operatorname{Im}\phi$.

The results may be summarized in a *commutative diagram:* any homomorphism $\phi : G \to L$ *factors* as $\phi = \mu \circ \gamma$ where γ is the canonical homomorphism with kernel $\ker\phi$. There are analogues in several other parts of mathematics; in particular, the rank–nullity theorem from linear algebra is of close kin.

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "\gamma"'] & & \operatorname{Im}\phi \\
& {}^{G}\!/_{\ker\phi} \arrow[ur, "\mu"'] &
\end{tikzcd}$$

Proof. The factor group exists since $\ker\phi \triangleleft G$ (Lemma 7.3). We check the isomorphism properties:

Well-definition and Bijectivity: These are immediate from Lemma 7.5 after writing $H = \ker\phi$:

$$g_1H = g_2H \iff \phi(g_1) = \phi(g_2) \iff \mu(g_1H) = \mu(g_2H)$$

Homomorphism: For all $g_1H, g_2H \in {}^{G}\!/_{H}$,

$$\begin{aligned}
\mu(g_1H \cdot g_2H) &= \mu(g_1g_2H) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) && (\phi \text{ is a homomorphism}) \\
&= \mu(g_1H)\mu(g_2H)
\end{aligned}$$

We conclude that μ is an isomorphism.

■

Examples 7.12. 1. Let $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{20}$ be the homomorphism $\phi(x) = 5x \,(\text{mod } 20)$ (Example 7.9). Its kernel and image are

$$\ker\phi = \big\{x \in \mathbb{Z}_{12} : 5x \equiv 0 \pmod{20}\big\} = \{0,4,8\} = \langle 4\rangle \le \mathbb{Z}_{12}$$
$$\operatorname{Im}\phi = \{5x \in \mathbb{Z}_{20} : x \in \mathbb{Z}_{12}\} = \{0,5,10,15\} = \langle 5\rangle \le \mathbb{Z}_{20}$$

The relevant factor group is

$$\mathbb{Z}_{12}/_{\ker\phi} = \Big\{\{0,4,8\},\{1,5,9\},\{2,6,10\},\{3,7,11\}\Big\} = \{\langle 4\rangle, 1+\langle 4\rangle, 2+\langle 4\rangle, 3+\langle 4\rangle\}$$

The canonical homomorphism γ and the isomorphism μ are

$$\gamma(x) = x + \langle 4\rangle \qquad \mu\big(x+\langle 4\rangle\big) = 5x$$

$$\begin{tikzcd} \mathbb{Z}_{12} \arrow[r, "\gamma"'] \arrow[rr, bend left, "\phi"] & \mathbb{Z}_{12}/_{\langle 4\rangle} \arrow[r, "\mu"'] & \operatorname{Im}\phi \\ x \arrow[r, mapsto] & x+\langle 4\rangle \arrow[r, mapsto] & 5x \end{tikzcd}$$

2. (Example 6.21.1) Let $H = \langle 2\pi\rangle \le \mathbb{R}$ and define $\phi : \mathbb{R} \to (\mathbb{C}^\times, \cdot)$ by $\phi(x) = e^{ix}$. This is a homomorphism with

$$\ker\phi = \{x \in \mathbb{R} : e^{ix} = 1\} = H \quad\text{and}\quad \operatorname{Im}\phi = S^1$$

The canonical homomorphism is

$$\gamma : \mathbb{R} \to \mathbb{R}/_H : x \mapsto x + \langle 2\pi\rangle$$

while the isomorphism we saw previously

$$\mu : \mathbb{R}/_H \to S^1 : x + \langle 2\pi\rangle \mapsto e^{ix}$$

is precisely that arising from the 1st isomorphism theorem.

3. The map $\phi : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ defined by $\phi(x,y) = 3x - 2y$ is a homomorphism. Moreover

$$\phi(x,y) = (0,0) \iff 3x = 2y \iff (x,y) = (2n,3n) \text{ for some } n \in \mathbb{Z}$$

We conclude that $\ker\phi = \langle(2,3)\rangle$. The canonical homomorphism is

$$\gamma : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}/_{\langle(2,3)\rangle} : (x,y) \mapsto (x,y) + \langle(2,3)\rangle$$

Since ϕ is surjective, we see that

$$\mathbb{Z}\times\mathbb{Z}/_{\langle(2,3)\rangle} \cong \mathbb{Z} \quad\text{via}\quad \mu\big((x,y)+\langle(2,3)\rangle\big) = 3x - 2y$$

With a little creativity, the theorem can be applied to the identification of factor groups: given $H \lhd G$, cook up a homomorphism $\phi : G \to L$ with $\ker\phi = H$, then $G/_H \cong \operatorname{Im}\phi$. We revisit some examples from the previous section in this context.

Examples (6.20, mk.II). Let $G = \mathbb{Z}_4 \times \mathbb{Z}_8$. For each subgroup H, we describe a homomorphism $\phi : G \to L$ with $\ker \phi = H$. There are many possible choices for ϕ; while ours will line up with what we saw in the original incarnation of these examples, hopefully you'll feel that the reasons for such choices are independent of our earlier discussion.

1. Given $H = \langle (0,1) \rangle$, we need a homomorphism where $\phi(0,1)$ is the identity. A simple way to do this is to ignore y and define

$$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_4 : (x,y) \mapsto x$$

This indeed has kernel $\ker \phi = \{(0,y) : y \in \mathbb{Z}_8\} = H$, whence

$$G/_H \cong \operatorname{Im} \phi = \mathbb{Z}_4$$

via the isomorphism $\mu : (x,y) + H \mapsto x$.

Note that μ is precisely the *inverse* of the isomorphism $\psi : x \mapsto (x,0) + H$ stated in the original version of this example; $(x,y) + H = (x,0) + H$ for this subgroup!

2. Given $H = \langle (0,2) \rangle$ we require $\phi(0,2)$ to be the identity. We may easily do this by taking y modulo 2 and defining

$$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_4 \times \mathbb{Z}_2 : (x,y) \mapsto (x,y)$$

This is a homomorphism with the correct kernel $\ker \phi = H$. Indeed ϕ is also surjective, whence

$$G/_H \cong \operatorname{Im} \phi = \mathbb{Z}_4 \times \mathbb{Z}_2$$

via the isomorphism $\mu\big((x,y) + H\big) = (x,y)$. Once again μ is the inverse of $\psi(x,y) = (x,y) + H$ in the original example.

3. If $H = \langle (2,4) \rangle = \{(0,0), (2,4)\}$, it is significantly trickier to find a suitable homomorphism. One approach is to observe that

$$(x,y) \in H \iff x \equiv 0 \pmod 2 \text{ and } y - 2x \equiv 0 \pmod 8$$

We therefore choose the homomorphism

$$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_2 \times \mathbb{Z}_8 : (x,y) \mapsto \big(x, y - 2x\big)$$

It is worth checking that this is well-defined: the $2x$ in the second factor is crucial! Certainly ϕ has the correct kernel. It is moreover surjective, e.g. $(p,q) = \phi(p, q + 2p)$, whence

$$G/_H \cong \operatorname{Im} \phi = \mathbb{Z}_2 \times \mathbb{Z}_8$$

via the isomorphism $\mu\big((x,y) + H\big) = (x, y - 2x)$.

Other homomorphisms are possible in all the above examples. This approach requires a little creativity! In general, it can be very difficult to *construct* a simple homomorphism with the correct kernel.

Exercises 7.2. Key concepts:

Canonical homomorphism $\gamma : G \to {}^{G}\!/_{H}$ *1^{st} isomorphism theorem* $\mu : {}^{G}\!/_{H} \cong \operatorname{Im}\phi$

1. Let $\phi : \mathbb{Z}_{18} \to \mathbb{Z}_{12}$ be the homomorphism $\phi(x) = 10x$.
   (a) Find the kernel of and image of ϕ.
   (b) List the elements of the factor group ${}^{\mathbb{Z}_{18}}\!/_{\ker\phi}$.
   (c) State an explicit isomorphism $\mu : {}^{\mathbb{Z}_{18}}\!/_{\ker\phi} \to \operatorname{Im}\phi$.
   (d) To what basic group $\mathbb{Z}_n$ is the factor group isomorphic?
2. Repeat the previous question for the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_{20} : x \mapsto 8x$.
3. For each function $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, find the kernel and identify the factor group ${}^{\mathbb{Z}\times\mathbb{Z}}\!/_{\ker\phi}$.
   (a) $\phi(x, y) = 3x + y$ (b) $\phi(x, y) = 2x - 4y$
4. (a) If a subgroup H of $G = \mathbb{Z}_{15} \times \mathbb{Z}_3$ has order 5, find its elements.
   (b) Show that $\phi(x, y) = (x, y)$ is a homomorphism $\phi : G \to \mathbb{Z}_3 \times \mathbb{Z}_3$ with $\ker\phi = H$.
   (c) What does the 1^{st} isomorphism theorem tell us about the factor group ${}^{G}\!/_{H}$?
5. Suppose G is a finite group with normal subgroup H and that $\phi : G \to L$ is a homomorphism with $\ker\phi = H$. Prove that $(G : H) \le |L|$ with equality if and only if ϕ is surjective.
6. Consider the map $\phi : \mathbb{Z} \times \mathbb{Z}_{12} \to \mathbb{Z}_3 \times \mathbb{Z}_6$ defined by
   $$\phi(x, y) = \big(2x + y, y\big)$$
   (a) Verify that ϕ is a well-defined homomorphism.
   (b) Compute $\ker\phi$ and identify the factor group ${}^{\mathbb{Z}\times\mathbb{Z}_{12}}\!/_{\ker\phi}$
7. Let $H = \langle(3, 1)\rangle \le G = \mathbb{Z}_9 \times \mathbb{Z}_3$. Find an explicit homomorphism $\phi : G \to \mathbb{Z}_9$ whose kernel is H, and thus identify the factor group ${}^{G}\!/_{H}$.
   (*Hint:* $(x, y) \in H = \{(0, 0), (3, 1), (6, 2)\} \iff \ldots$)
8. Consider $H = \langle(3, 3)\rangle \le G = \mathbb{Z}_9 \times \mathbb{Z}_9$. Find a surjective homomorphism $\phi : G \to \mathbb{Z}_3 \times \mathbb{Z}_9$ whose kernel is H and hence prove that ${}^{G}\!/_{H} \cong \mathbb{Z}_3 \times \mathbb{Z}_9$.
9. Let $\phi : S^1 \to S^1 : z \mapsto z^2$.
   (a) Find the kernel of ϕ and describe the canonical homomorphism $\gamma : S_1 \to {}^{S^1}\!/_{\ker\phi}$.
   (b) What does the first isomorphism theorem say about the factor group ${}^{S^1}\!/_{\ker\phi}$.
   (c) For each n, identify the factor group ${}^{S^1}\!/_{U_n}$, where U_n is the group of n^{th} roots of unity.

7.3 Conjugation, Cycle Types, Centers and Automorphisms

In this section we consider an important type of homomorphism and some its consequences.

Definition 7.13. Let G be a group and $x, y \in G$. We say that y is *conjugate to* x if

$$\exists g \in G \quad \text{such that} \quad y = gxg^{-1}$$

If $g \in G$ is fixed, then *conjugation by* g is the map $c_g : G \to G : x \mapsto gxg^{-1}$.

We've met this notion before: recall that a subgroup H is normal if and only if $c_g(h) \in H$ for all $g \in G$ (Corollary 6.7). It should also be familiar from linear algebra, in the form of *similarity*. Recall that square matrices A, B are similar if $B = MAM^{-1}$ for some invertible M. Such matrices have the same eigenvalues and, essentially, 'do the same thing' with respect to different bases. An explicit group theory analogue of this is Theorem 7.17 below.

Lemma 7.14. *Conjugation by g is a isomorphism $c_g : G \cong G$.*

Proof. Conjugation by g^{-1} is the inverse function of c_g^{-1}:

$$c_{g^{-1}}(c_g(x)) = g^{-1}gxg^{-1}(g^{-1})^{-1} = x, \quad \text{etc.}$$

We moreover have a homomorphism:

$$c_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = c_g(x)c_g(y)$$

■

Lemma 7.15. *Conjugacy is an equivalence relation $(x \sim y \iff \exists g \in G$ such that $y = gxg^{-1})$.*

The proof is an exercise. The equivalence classes under conjugacy are termed *conjugacy classes.*

Examples 7.16.
1. If G is abelian then every conjugacy class contains only one element:

$$x \sim y \iff \exists g \in G \quad \text{such that} \quad y = gxg^{-1} = xgg^{-1} = x$$

2. The smallest non-abelian group is S_3 has conjugacy classes

$$\{e\}, \quad \{(1\,2), (1\,3), (2\,3)\}, \quad \{(1\,2\,3), (1\,3\,2)\}$$

This can be computed directly, but it follows immediately from...

Theorem 7.17. *The conjugacy classes of S_n are the* cycle types*: elements are conjugate if and only if they have the same cycle type.*

If an element $\sigma \in S_n$ is written as a product of disjoint cycles, then its cycle type is clear. For instance:

- $(1\,2\,3)(4\,5)$ has the same cycle type as $(1\,5\,6)(2\,3)$: we might call these 3,2-cycles.
- $(1\,2)(3\,4)$ has a different cycle type; 2,2.

Before seeing the proof it is beneficial to try an example.

Example 7.18. If $\rho = (2\,4\,3)$ and $\sigma = (1\,2)(3\,4)$ in S_4, then

$$\rho\sigma\rho^{-1} = (2\,4\,3)(1\,2)(3\,4)(2\,3\,4) = (1\,4)(2\,3)$$

Not only does this have the same cycle type as σ, but if may be obtained simply by applying ρ to the entries of σ!

$$\rho\sigma\rho^{-1} = (1\,4)(2\,3) = \big(\rho(1)\,\rho(2)\big)\big(\rho(3)\,\rho(4)\big)$$

This also tells us how to reverse the process: given 2,2-cycles $\sigma = (1\,2)(3\,4)$ and $\tau = (1\,4)(2\,3)$ simply place σ on top of τ in a table to define a suitable $\rho = (2\,4\,3)$ for which $\rho\sigma\rho^{-1} = \tau$.

x	1	2	3	4
$\rho(x)$	1	4	2	3

The proof is nothing more than the example done abstractly!

Proof. ($\Rightarrow$) We consider conjugation by $\rho \in S_n$. First let $\sigma = (a_1 \cdots a_k)$ be a k-cycle and write

$$A = \{a_1, \ldots, a_k\}, \qquad R = \{\rho(a_1), \ldots, \rho(a_k)\}$$

Since ρ is a bijection, $|R| = k$ are distinct and $x \in R \iff \rho^{-1}(x) \in A$. There are two cases:

If $x \in R$: Let $x = \rho(a_j)$, then

$$\rho\sigma\rho^{-1}\big(\rho(a_j)\big) = \rho\sigma(a_j) = \rho(a_{j+1})$$

where a_{k+1} is understood to be a_1.

If $x \notin R$: Since $\rho^{-1}(x) \notin A$ it is unmoved by σ, whence

$$\rho\sigma\rho^{-1}(x) = \rho\sigma(\rho^{-1}(x)) = \rho\rho^{-1}(x) = x$$

We conclude that $\rho\sigma\rho^{-1} = \big(\rho(a_1) \cdots \rho(a_k)\big)$ is also a k-cycle!

More generally, if $\sigma = \sigma_1 \cdots \sigma_l$ is a product of disjoint cycles, then

$$\rho\sigma\rho^{-1} = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1}) \cdots (\rho\sigma_l\rho^{-1})$$

has the same cycle type as σ.

($\Leftarrow$) Suppose $\sigma = \sigma_1 \cdots \sigma_l$ and $\tau = \tau_1 \cdots \tau_l \in S_n$ have the same cycle type, written so that the corresponding orbits have the same length. Moreover, assume we've included all necessary 1-cycles so that $\bigcup \sigma_i = \{1, \ldots, n\} = \bigcup \tau_i$. Define a permutation ρ by writing the orbits of σ and τ on top each other

x	σ_1	σ_2	$\cdots$	σ_l
$\rho(x)$	τ_1	τ_2	$\cdots$	τ_l

If $s_{i,j}$ and $t_{i,j}$ are the j^{th} elements of the orbits σ_i and τ_i, then

$$\rho\sigma\rho^{-1}(t_{i,j}) = \rho\sigma(s_{i,j}) = \rho\big(s_{i,j+1}\big) = t_{i,j+1} = \tau\big(t_{i,j}\big)$$

We conclude that $\rho\sigma\rho^{-1} = \tau$, as required. ∎

Examples 7.19. 1. The permutations $\sigma = (1\,4\,5)(2\,7\,6)$ and $\tau = (1\,6\,5)(3\,4\,7)$ in S_7 are conjugate: the table defines a suitable ρ.

$$\begin{array}{c|ccccccc} x & 1 & 4 & 5 & 2 & 7 & 6 & 3 \\ \hline \rho(x) & 1 & 6 & 5 & 3 & 4 & 7 & 2 \end{array} \implies \rho = (2\,3)(4\,6\,7)$$

Indeed

$$\rho\sigma\rho^{-1} = (2\,3)(4\,6\,7)(1\,4\,5)(2\,7\,6)(2\,3)(4\,7\,6) = (1\,6\,5)(3\,4\,7) = \tau$$

There are other possible choices of ρ; just write the orbits of σ, τ in different orders.

2. (Example 6.3.2) We've checked previously that $V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a normal subgroup of A_4. It is moreover a normal subgroup of S_4: since V contains the identity and all 2,2-cycles it is closed under conjugacy and thus a normal subgroup of both A_4 and S_4.

Automorphisms

We've already seen that conjugation $c_g : G \to G$ by a fixed element is an isomorphism. We now consider all such maps.

Definition 7.20. An *automorphisms* of a group G is an isomorphism of G with itself. The set of such is denoted $\operatorname{Aut} G$. The *inner automorphisms* are the conjugations

$$\operatorname{Inn} G = \{c_g : G \to G \text{ where } c_g(x) = gxg^{-1}\}$$

Example 7.21. There are four homomorphisms $\phi_k : \mathbb{Z}_4 \to \mathbb{Z}_4$ (Corollary 7.8);

$$\phi_0(x) = 0, \quad \phi_1(x) = x, \quad \phi_2(x) = 2x, \quad \phi_3(x) = 3x$$

of which two are automorphisms: $\operatorname{Aut} \mathbb{Z}_4 = \{\phi_1, \phi_3\}$. Observe that ϕ_1 is the identity function and that $\phi_3 \circ \phi_3 = \phi_1$. The automorphisms therefore comprise a *group* (necessarily isomorphic to $\mathbb{Z}_2$) under composition of functions.

As for conjugations, observe that for any $g \in \mathbb{Z}_4$,

$$c_g(x) = g + x + (-g) = x$$

since $\mathbb{Z}_4$ is abelian. There is only one inner automorphism of $\mathbb{Z}_4$, the identity function ϕ_1.

Hunting for automorphisms can be difficult. Here is a helpful observation for narrowing things down; the proof is an exercise.

Lemma 7.22. *If $\phi \in \operatorname{Aut} G$ and $x \in G$, then the orders of x and $\phi(x)$ are identical.*

This helps to streamline the previous example: $\phi(1)$ must have the same order (four) as 1 and so our only possibilities are $\phi(1) = 1$ or $\phi(1) = 3$. These possibilities generate the two observed automorphisms.

Example 7.23. We describe all automorphisms ϕ of S_3. Consider $\sigma = (1\,2)$ and $\tau = (1\,2\,3)$. Since the order of an element is preserved by ϕ, we conclude that

$$\phi(e) = e, \quad \phi(\sigma) \in \{(1\,2), (1\,3), (2\,3)\}, \quad \phi(\tau) \in \{(1\,2\,3), (1\,3\,2)\}$$

We therefore have a maximum of *six* possible automorphism; it is tedious to check, but *all* really do define automorphisms! Indeed all may be explicitly realized as conjugations whence $\operatorname{Aut} S_3 = \operatorname{Inn} S_3$. Here is the data; verify some of it for yourself:

element g	$c_g(e)$	$c_g(1\,2)$	$c_g(1\,3)$	$c_g(2\,3)$	$c_g(1\,2\,3)$	$c_g(1\,3\,2)$
e	e	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,2)$	e	$(1\,2)$	$(2\,3)$	$(1\,3)$	$(1\,3\,2)$	$(1\,2\,3)$
$(1\,3)$	e	$(2\,3)$	$(1\,3)$	$(1\,2)$	$(1\,3\,2)$	$(1\,2\,3)$
$(2\,3)$	e	$(1\,3)$	$(1\,2)$	$(2\,3)$	$(1\,3\,2)$	$(1\,2\,3)$
$(1\,2\,3)$	e	$(2\,3)$	$(1\,2)$	$(1\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,3\,2)$	e	$(1\,3)$	$(2\,3)$	$(1\,2)$	$(1\,2\,3)$	$(1\,3\,2)$

As the next result shows, the automorphisms again form a group under composition, in this case a group of order 6 which is easily seen to be *non-abelian*: for instance

$$c_{(1\,2)}c_{(1\,3)} = c_{(1\,3\,2)} \neq c_{(1\,2\,3)} = c_{(1\,3)}c_{(1\,2)}$$

By process of elimination, we conclude that $\operatorname{Aut} S_3 \cong S_3$.

Theorem 7.24. *$\operatorname{Aut} G$ and $\operatorname{Inn} G$ are groups under composition. Moreover $\operatorname{Inn} G \lhd \operatorname{Aut} G$.*

Proof. That $\operatorname{Aut} G$ is a group is simply the fact that composition and inverses of isomorphisms are isomorphisms: you should already have made this argument when answering Exercise 2.3.13. By Lemma 7.14, every conjugation is an isomorphism, and it is simple to check that $c_g \circ c_h = c_{gh}$ and $c_g^{-1} = c_{g^{-1}}$: we conclude that $\operatorname{Inn} G \subseteq \operatorname{Aut} G$.
For normality, we check that $\operatorname{Inn} G$ is closed under conjugation! Let $\tau \in \operatorname{Aut} G$ and $c_g \in \operatorname{Inn} G$. For any $x \in G$, we have[22]

$$\begin{aligned}
(\tau c_g \tau^{-1})(x) &= \tau\Big(c_g\big(\tau^{-1}(x)\big)\Big) && \text{(definition of } c_g\text{)}\\
&= \tau\Big(g\big(\tau^{-1}(x)\big)g^{-1}\Big)\\
&= \Big(\tau(g)\Big)\Big(\tau\big(\tau^{-1}(x)\big)\Big)\Big(\tau(g^{-1})\Big) && \text{(since } \tau \text{ is a homomorphism)}\\
&= \big(\tau(g)\big)x\big(\tau(g)\big)^{-1} && \text{(again since } \tau \text{ is an homomorphism)}\\
&= c_{\tau(g)}(x)
\end{aligned}$$

We conclude that $\tau c_g \tau^{-1} = c_{\tau(g)} \in \operatorname{Inn} G$, from which $\operatorname{Inn} G \lhd \operatorname{Aut} G$. ■

[22] The challenge in reading the proof is simply to keep track of where everything lives. To help, the inverse symbol is colored: τ^{-1} means the inverse *function*, whereas g^{-1} means the inverse of an *element* in G.

Centers

We say that an element g in a group G *commutes* with another element $x \in G$ if the order of multiplication is irrelevant: i.e. if $gx = xg$. Otherwise said, if $c_g(x) = x$. It natural to ask whether there are any elements which commute with *all others*. There are two very simple cases:

- If G is abelian, then every element commutes with every other element!
- The identity e commutes with everything, regardless of G.

In general, the set of such elements will fall somewhere between these extremes. This subset will turn out to be another normal subgroup of G.

Definition 7.25. The *center* of a group G is the subset of G which commutes with everything in G:

$$Z(G) := \{g \in G : \forall h \in G,\ gh = hg\}$$

We will prove that $Z(G) \triangleleft G$ shortly. First we give a few examples; unless G is abelian, the center is typically difficult to compute, so we omit more of the details.

Examples 7.26. 1. $Z(G) = G \iff G$ is abelian.

2. $Z(S_n) = \{e\}$ if $n \geq 3$. This is straightforward to check when $n = 3$ since there are only six elements. In general, think about the proof of Theorem 7.17...

3. $Z(D_{2n+1}) = \{e\}$ and $Z(D_{2n}) = \{e, \rho_{n/2}\}$, where $\rho_{n/2}$ is rotation by $180°$. For instance, it is easy to see in D_{2n+1} that any rotation and reflection fail to commute.

4. $Z\big(\mathrm{GL}_n(\mathbb{R})\big) = \{\lambda I_n : \lambda \in \mathbb{R}^\times\}$. If you've done enough linear algebra, an argument is reasonably straightforward (Exercise 12)

Theorem 7.27. *For any group G:*

1. $Z(G) \triangleleft G$
2. ${}^{G}\!/_{Z(G)} \cong \operatorname{Inn} G$

Proof. 1. The function $\phi : G \to \operatorname{Inn} G$ defined by $\phi(g) = c_g$ is a homomorphism:

$$\begin{aligned} &c_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = c_g(c_h(x)) \\ \implies &\phi(gh) = \phi(g)\phi(h) \end{aligned}$$

Now observe that

$$g \in \ker\phi \iff \forall x \in G,\ c_g(x) = gxg^{-1} = x \iff g \in Z(G)$$

from which $\ker\phi = Z(G)$ is a normal subgroup of G.

2. Since ϕ is surjective, the 1$^{\text{st}}$ isomorphism theorem tells us that

$${}^{G}\!/_{Z(G)} \cong \operatorname{Im}\phi = \operatorname{Inn} G$$

■

Exercises 7.3. Key concepts:

Conjugation *conjugacy classes* *cycle types are conjugacy classes in S_n*
(inner) automorphism *center of a group*

1. Either find some $\rho \in G$ such that $\rho\sigma\rho^{-1} = \tau$, or explain why no such element exists:
   (a) $\sigma = (1\,2\,3)$, $\tau = (1\,3\,2)$ where $G = S_3$.
   (b) $\sigma = (1\,4\,5\,6)(2\,3)(5\,6)$, $\tau = (1\,2\,3\,4)(5\,6)(2\,6)$ where $G = S_6$.
   (c) $\sigma = (1\,4\,5\,6)(2\,3)(5\,6)$, $\tau = (1\,2)(3\,5\,6)$ where $G = S_6$.
2. Recall Example 7.19.1. Find another element $\nu \neq \rho$ for which $\nu\sigma\nu^{-1} = \tau$.
3. Prove Lemma 7.15. Prove that the relation

   $$x \sim y \iff y \text{ is conjugate to } x$$

   is an equivalence relation on any group G.
4. (a) Suppose y is conjugate to x in a group G. Prove that the orders of x and y are identical.
   (b) Show that the converse to part (a) is *false* by exhibiting two non-conjugate elements of the same order in some group.
5. Let $H \leq G$, fix $a \in G$ and define the *conjugate subgroup* $K = c_a(H) = \{aha^{-1} : h \in H\}$.
   (a) Prove that K is indeed a subgroup of G.
   (b) Prove that the function $\psi : H \to K : h \mapsto aha^{-1}$ is an isomorphism of groups.
   (c) If $H \triangleleft G$, what can you say about $c_a(H)$?
   (d) Let $H = \{e, (1\,2)\} \leq S_3$ and $a = (1\,2\,3)$. Compute the conjugate subgroup $K = c_a(H)$.
6. We've already seen that $V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a normal subgroup of S_4.
   (a) Show that *normal subgroup* is not transitive by giving an example of a normal subgroup $K \triangleleft V$ which is *not normal* in S_4.
   (b) How many *other* subgroups does S_4 have which are isomorphic to V? Why are none of them normal in S_4?
   (c) Explain why ${}^{S_4}/_{V}$ is a group of order six. Prove that

   $$(1\,2)V(1\,3)V \neq (1\,3)V(1\,2)V$$

   Hence conclude that ${}^{S_4}/_{V} \cong S_3$.
   (d) Why is it obvious that the following six left cosets are distinct.

   $$V,\ (1\,2)V,\ (1\,3)V,\ (2\,3)V,\ (1\,2\,3)V,\ (1\,3\,2)V$$

   (*Hint: Think about how none of the representatives a of the above cosets move the number 4 and consider* $aV = bV \iff b^{-1}a \in V \ldots$)
   (e) Define an isomorphism $\mu : {}^{S_4}/_{V} \to S_3$ and prove that it is an isomorphism.

7. Prove Lemma 7.22: if $\phi \in \operatorname{Aut} G$ and $x \in G$, then $\phi(x)$ has the same order as x.
8. Describe all automorphisms of the Klein four-group V.
   (*Hint: use the previous question!*)
9. Recall Exercise 7.1.6. Explain why $\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^\times$.
   (*Hint: consider $\phi_k(x) = kx$ where $\gcd(k,n) = 1$ and map $\psi : k \mapsto \phi_k$*)
10. Let G be a group. Prove directly that $Z(G) \lhd G$, *without* using Theorem 7.27. That is:
    (a) Prove that $Z(G)$ is closed under the group operation and inverses.
    (b) Prove that $gZ(G) = Z(G)g$ for all $g \in G$.
11. Suppose $n \geq 3$ and that $\sigma \in Z(S_n)$.
    (a) By considering $\sigma(1\,2)\sigma^{-1}$, prove that $\{\sigma(1), \sigma(2)\} = \{1, 2\}$.
    (b) If $\sigma(1) = 2$, repeat the calculation with $\sigma(1\,3)\sigma^{-1}$ to obtain a contradiction.
    (c) Hence, or otherwise, deduce that $Z(S_n) = \{e\}$.
12. We identify the center of the general linear group.

    The $n \times n$ matrix $A = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & & & 0 \\ 0 & 0 & 0 & & & 0 \\ \vdots & & & \ddots & \ddots & \\ 0 & 0 & 0 & & 0 & 1 \\ 0 & 0 & 0 & \cdots & & 0 \end{pmatrix}$ has a single one-dimensional eigenspace: $A\mathbf{e}_1 = \mathbf{0}$.

    (a) Let $B \in Z\big(\mathrm{GL}_n(\mathbb{R})\big)$. Use the fact that $AB = BA$ to prove that $B\mathbf{e}_1 = \lambda\mathbf{e}_1$ for some $\lambda \neq 0$.
    (b) Let $\mathbf{x} \in \mathbb{R}^n$ be non-zero and X an invertible matrix for which $X\mathbf{e}_1 = \mathbf{x}$ (e.g. put $\mathbf{x}$ in the 1^{st} column of X). Prove that $B\mathbf{x} = \lambda\mathbf{x}$.
    (c) Since the observation in part (b) holds for *any* $\mathbf{x} \in \mathbb{R}^n$, what can we conclude about B? What is the group $Z\big(\mathrm{GL}_n(\mathbb{R})\big)$?
13. (a) Prove that D_4 has center $Z(D_4) = \{e, \rho_2\}$, where ρ_2 is rotation by $180°$.
    (b) State the cosets of $Z(D_4)$. What is the order of each? Determine whether ${}^{D_4}\!/_{Z(D_4)}$ is isomorphic to $\mathbb{Z}_4$ or to the Klein four-group V.
    (c) (Hard) Can you find a homomorphism $\phi : D_4 \to D_4$ whose kernel is $Z(D_4)$?
    (*Hint: draw a picture and think about doubling angles of rotation and reflection!*)

8 Group Actions

8.1 Group Actions, Fixed Sets and Isotropy Subgroups

In this final chapter, we revisit a central idea: groups are interesting and useful often because of how they *transform sets*. Recall how the symmetric group S_n was defined in terms of what its elements do to the set $\{1, \ldots, n\}$. This is an example of a general situation.

Definition 8.1. A group G *acts*[23] on a set X via a map $\cdot : G \times X \to X$ if,

(a) $\forall x \in X,\ e \cdot x = x,$ and,

(b) $\forall x \in X,\ g, h \in G,\ g \cdot (h \cdot x) = (gh) \cdot x.$

Part (b) says $g \mapsto g\cdot$ is a homomorphism of *binary structures* (the functions $X \to X$ needn't form a group).

Examples 8.2. 1. The symmetric S_n group acts on $X = \{1, 2, \ldots, n\}$. As a sanity check:

   (a) $e(x) = x$ for all $x \in \{1, \ldots, n\}$.
   (b) $\sigma\big(\tau(x)\big) = (\sigma\tau)(x)$ is composition of functions!

2. Any group G acts on itself by left multiplication. This is essentially Cayley's Theorem (5.8). It also acts on itself by conjugation ($c_g \circ c_h = c_{gh}$ is Theorem 7.24).

3. If X is the set of orientations of a regular n-gon such that one vertex is at $(1, 0)$ and the center is at $(0, 0)$, then D_n acts on X by rotations and reflections. Note that X has cardinality $2n$.

4. Matrix groups act on vector spaces by matrix multiplication. For example the orthogonal group $\mathrm{O}_2(\mathbb{R})$ can be seen to transform vectors via rotations and reflections.

$$\mathrm{O}_2(\mathbb{R}) \times \mathbb{R}^2 \to \mathbb{R}^2 : (A, \mathbf{v}) \mapsto A\mathbf{v}$$

5. A group can act on many different sets. Here are three further actions of the orthogonal group:

   i. $\mathrm{O}_2(\mathbb{R})$ acts on the set $X = \{1, -1\}$ via $A \cdot x := (\det A)x$.
   ii. $\mathrm{O}_2(\mathbb{R})$ acts on the set $X = \mathbb{R}^3$ via $A \cdot \mathbf{v} := A(v_1\mathbf{i} + v_2\mathbf{j}) + v_3\mathbf{k}$.
   iii. $\mathrm{O}_2(\mathbb{R})$ acts on the unit circle $X = S^1 \subseteq \mathbb{R}^2$ via matrix multiplication $A \cdot \mathbf{v} := A\mathbf{v}$.

We often use an action to visualize a group; in this context, some actions are better than others. Consider the three actions of $\mathrm{O}_2(\mathbb{R})$ in part 5 above:

i. The set X is very small. Many matrices act in exactly the same way so the action is an unhelpful means of visualizing the group.
ii. The set X feels too large. The action leaves any vertical vector untouched.
iii. The circle $X = S^1$ is large enough so that the action of distinct matrices can be distinguished without being inefficiently large.[24]

[23]This is really a *left* action. There is an analogous definition of a *right action*. In this course, all actions will be left.
[24]A *Goldilocks* action, perhaps?

These notions can be formalized.

Definition 8.3. Let $G \times X \to X$ be an action.

1. The *fixed set* of $g \in G$ is the set
$$\mathrm{Fix}(g) := \{x \in X : g \cdot x = x\} \qquad \text{(also written } X_g\text{, though we won't do this)}$$
2. The *isotropy subgroup* or *stabilizer* of $x \in X$ is the set
$$\mathrm{Stab}(x) := \{g \in G : g \cdot x = x\} \qquad \text{(also written } G_x\text{)}$$
3. The action is *faithful* if the only element of G which fixes everything is the identity. This can be stated in two equivalent ways:

   (a) $\mathrm{Fix}(g) = X \iff g = e$ (b) $\bigcap_{x \in X} \mathrm{Stab}(x) = \{e\}$
4. The action is *transitive* if any element of X may be transformed to any other:
$$\forall x, y \in X,\ \exists g \in G \text{ such that } y = g \cdot x$$

Examples (8.2 cont). 1. The action of S_n on $\{1, 2, \ldots, n\}$ is both faithful and transitive:

   Faithful: if $\sigma(x) = x$ for all $x \in \{1, 2, \ldots, n\}$, then $\sigma = e$.

   Transitive: if $x \neq y$, then the 2-cycle $(x\, y)$ maps $x \mapsto y$.

2. The action of a group on itself by left multiplication is both faithful and transitive. Conjugation is more complex: in most situations it is neither.
3. D_n acts faithfully and transitively on the orientations of the n-gon.
4. The action of $\mathrm{O}_2(\mathbb{R})$ on $\mathbb{R}^2$ is faithful but not transitive: for instance the zero vector cannot be transformed into any other vector so $\mathrm{Stab}(\mathbf{0}) = \mathrm{O}_2(\mathbb{R})$.
5. We leave these as exercises.

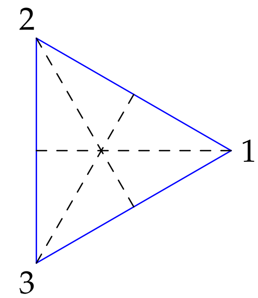
Lemma 8.4. *For each $x \in X$, the stabilizer $\mathrm{Stab}(x)$ is indeed a subgroup of G.*

Proof. $\mathrm{Stab}(x)$ is a non-empty subset of G since $e \in \mathrm{Stab}(x)$. It sufficient to show that it is closed under multiplication and inverses. Let $g, h \in \mathrm{Stab}(x)$, then
$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x \implies gh \in \mathrm{Stab}(x)$$
Moreover
$$x = g \cdot x \implies g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$
■

Example 8.5. The dihedral group $D_3 = \{e, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ acts on the set X of vertices of an equilateral triangle.[25] The fixed sets and stabilizers for this action are as follows:

Element g	$\mathrm{Fix}(g)$
e	$\{1,2,3\}$
ρ_1	$\emptyset$
ρ_2	$\emptyset$
μ_1	$\{1\}$
μ_2	$\{2\}$
μ_3	$\{3\}$

Vertex x	$\mathrm{Stab}(x)$
1	$\{e, \mu_1\}$
2	$\{e, \mu_2\}$
3	$\{e, \mu_3\}$



D_3 also acts on the set of *edges* of the triangle $Y = \{\{1,2\}, \{1,3\}, \{2,3\}\}$. You needn't write all these out since, by the symmetry of the triangle, stabilizing an edge is equivalent to stabilizing its opposite vertex. Still, here is the data:

Element g	$\mathrm{Fix}(g)$
e	$\{1,2,3\}$
ρ_1	$\emptyset$
ρ_2	$\emptyset$
μ_1	$\{\{2,3\}\}$
μ_2	$\{\{1,3\}\}$
μ_3	$\{\{1,2\}\}$

Edge $\{x,y\}$	$\mathrm{Stab}(\{x,y\})$
$\{1,2\}$	$\{e, \mu_3\}$
$\{1,3\}$	$\{e, \mu_2\}$
$\{2,3\}$	$\{e, \mu_1\}$

Exercises 8.1. Key concepts:

(left) action $\quad \mathrm{Fix}(g) \quad \mathrm{Stab}(x) \le G \quad$ *faithful/transitive actions*

1. For part 5 of Example 8.2, determine whether each action is faithful and/or transitive.
2. Let $G = \langle \sigma \rangle \le S_6$ where $\sigma = (1\,2\,3\,4\,5\,6)$. G acts on the set $X = \{1,2,3,4,5,6\}$ in a natural way.
   (a) State the fixed sets and stabilizers for this action.
   (b) Is the action of G faithful? Transitive?
3. Repeat the previous question when $\sigma = (1\,3)(2\,4\,6)$.
4. Mimic Example 8.5 for the actions of D_4 on $X = \{\text{vertices}\}$ and $Y = \{\text{edges}\}$ of the square. (*Use whatever notation you like; ρ, μ, δ or cycle notation*)
5. Suppose G acts on X.
   (a) Let $Y \subseteq X$ and define $\mathrm{Stab}\,Y = \{g \in G : \forall y \in Y, g \cdot y = y\}$. Prove that $\mathrm{Stab}\,Y$ is a subgroup of G.
   (b) Let G act on itself by conjugation ($X = G$!). What is another name for the subgroup $\mathrm{Stab}\,G$?
6. Suppose G has a left action on X. Prove that G acts faithfully on X if and only if no two distinct elements of G have the same action on every element.

[25]Recall that ρ_1 rotates 120° counter-clockwise, that $\rho_2 = \rho_1^2$ and that μ_i reflects across the altitude through vertex i.

8.2 Orbits & Burnside's Formula

We first encountered orbits in the context of the symmetric groups S_n. The same idea applies to any action.

Definition 8.6. Let $G \times X \to X$ be an action. The *orbit* of $x \in X$ under G is the set of elements into which x may be transformed:

$$Gx = \{g \cdot x : g \in G\} \subseteq X$$

Examples 8.7. 1. If $X = \{1, 2, \ldots n\}$ and $G = \langle \sigma \rangle \leq S_n$, then

$$Gx = \{\sigma^k(x) : k \in \mathbb{Z}\} = \mathrm{orb}_x(\sigma)$$

The definition of orbits therefore coincides with that seen earlier in the course.

2. A transitive *action*[26] has only one orbit.

3. If $O_2(\mathbb{R})$ acts on $\mathbb{R}^2$ by matrix multiplication, then the orbits are circles centered at the origin!

Lemma 8.8. *The orbits of an action partition X.*

Since this is almost identical to the corresponding result for orbits in S_n (Theorem 5.11), we leave the proof as an exercise.

Our next result is analogous to Lemma 7.5, where we counted the number of (left) cosets of $\ker \phi$.

Lemma 8.9. *The cardinality of the orbit Gx is the index of the isotropy subgroup* $\mathrm{Stab}(x)$*:*

$$|Gx| = (G : \mathrm{Stab}(x))$$

Proof. Observe that

$$g \cdot x = h \cdot x \iff h^{-1}g \cdot x = x \iff h^{-1}g \in \mathrm{Stab}(x) \iff g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x)$$

The contrapositive says that distinct elements of the orbit Gx correspond to distinct left cosets. ∎

Example 8.10. Let $\sigma = (1\,4)(2\,7\,3) \in S_7$. Consider $X = \{1, 2, 3, 4, 5, 6, 7\}$ under the action of the cyclic group $G = \langle \sigma \rangle$. The orbits are precisely the disjoint cycles: $\{1, 4\}$, $\{2, 3, 7\}$, $\{5\}$, $\{6\}$. Observe that G has six elements:

$$e, \quad \sigma = (1\,4)(2\,7\,3), \quad \sigma^2 = (2\,3\,7), \quad \sigma^3 = (1\,4), \quad \sigma^4 = (2\,7\,3), \quad \sigma^5 = (1\,4)(2\,3\,7)$$

The Lemma is easily verifiable: for instance if $x = 3$,

$$\mathrm{Stab}(x) = \{\tau \in G : \tau(3) = 3\} = \{\sigma^k : \sigma^k(3) = 3\} = \{e, \sigma^3\}$$
$$\implies (G : \mathrm{Stab}(x)) = \frac{6}{2} = 3 = |\{2, 3, 7\}| = |Gx|$$

[26] Unhelpfully, we now have two meanings of *transitive*; one for equivalence relations and one for actions.

It is often useful to count the *number* of orbits of an action. For *finite* actions, this turns out to be possible in two different ways.

Theorem 8.11 (Burnside's formula). *Let G be a finite group acting on a finite set X. Then the number of orbits in X under G satisfies*

$$\#\,\text{orbits} = \frac{1}{|G|}\sum_{x\in X}|\text{Stab}(x)| = \frac{1}{|G|}\sum_{g\in G}|\text{Fix}(g)|$$

Proof. By Lemma 8.9, It follows that

$$\frac{1}{|G|}\sum_{x\in X}|\text{Stab}(x)| = \sum_{x\in X}\frac{|\text{Stab}(x)|}{|G|} = \sum_{x\in X}\frac{1}{(G:\text{Stab}(x))} = \sum_{x\in X}\frac{1}{|Gx|}. \qquad (*)$$

Consider a fixed orbit Gy. Since $|Gx| = |Gy|$ for each $x \in Gy$, we see that

$$\sum_{x\in Gy}\frac{1}{|Gx|} = \frac{|Gy|}{|Gy|} = 1$$

The sum $(*)$ therefore counts 1 for each distinct orbit in X and therefore returns the number of orbits.

For the second equality, observe that

$$S = \{(g,x) \in G\times X : g\cdot x = x\}$$

has cardinality

$$|S| = \sum_{x\in X}|\text{Stab}(x)| = \sum_{g\in G}|\text{Fix}(g)|$$

■

Example (8.10 cont). When $G = \langle\sigma\rangle = \langle(1\,4)(2\,7\,3)\rangle$ acts on $X = \{1,2,3,4,5,6,7\}$, the stabilizers and fixed sets are as follows:

$x \in X$	$\text{Stab}(x)$
1	$\{e,\sigma^2,\sigma^4\}$
2	$\{e,\sigma^3\}$
3	$\{e,\sigma^3\}$
4	$\{e,\sigma^2,\sigma^4\}$
5	$G = \{e,\sigma,\sigma^2,\sigma^3,\sigma^4,\sigma^5\}$
6	G
7	$\{e,\sigma^3\}$

$g \in G$	$\text{Fix}(g)$
e	$X = \{1,2,3,4,5,6,7\}$
σ	$\{5,6\}$
σ^2	$\{1,4,5,6\}$
σ^3	$\{2,3,5,6,7\}$
σ^4	$\{1,4,5,6\}$
σ^5	$\{5,6\}$

Burnside's formula just sums the number of elements in all of the subsets in the right column of each table:

$$\begin{aligned}4 = \#\,\text{orbits} &= \frac{1}{|G|}\sum_{x\in X}|\text{Stab}(x)| = \frac{1}{6}(3+2+2+3+6+6+2)\\ &= \frac{1}{|G|}\sum_{g\in G}|\text{Fix}(g)| = \frac{1}{6}(7+2+4+5+4+2)\end{aligned}$$

One reason to count the number of orbits of an action is that we often want to consider objects as equivalent if they differ by the action of some simple group.

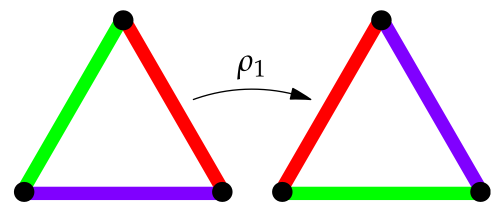
Example 8.12. A child's toy consists of a wooden equilateral triangle where the edges are to be painted using any choice of colors from the rainbow. How many distinct toys could we create?

There are two problems: we need to describe the variety of possible toys, and we need to know what *distinct* means!

We use group actions to address both problems:

- A toy may be considered as a subset of $X = \{\text{painted triangles}\} = \{\text{ordered color triples}\}$. Since there are 7 choices for the color of each edge, we see that $|X| = 7^3 = 343$ is a large set!
- Two toys are equivalent if they differ by a rotation in 3-dimensions. This amount to the natural action of D_3 on X: for instance

$$\rho_1 \cdot (\text{red,green,violet}) = (\text{violet,red,green})$$



The number of orbits is the number of distinct toys, which we may compute using Burnside. Since it would be time consuming to compute the stabilizer of each element of X, we use the fixed set approach.

- Identity e: Plainly $\text{Fix}(e) = X$, since e leaves every coloring unchanged.
- Rotations ρ_1, ρ_2: If a color-scheme is fixed by ρ_j, then all pairs of adjacent edges must be the same color. The only color-schemes fixed by ρ_j are those where all sides have the same color, whence $|\text{Fix}(\rho_i)| = 7$.
- Reflections μ_1, μ_2, μ_3: Since μ_j swaps two edges, anything in its fixed set must have these edges the same. We have 7 choices for the color of the switched edges, and an independent choice of 7 colors for the other edge, whence $\left|\text{Fix}(\mu_j)\right| = 7^2 = 49$.

The number of distinct toys is therefore

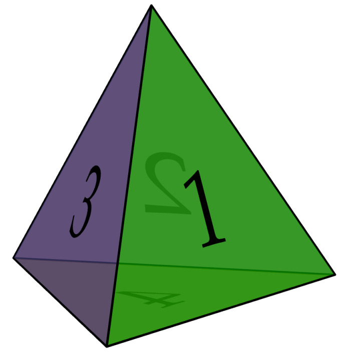
$$\begin{aligned}
\#\text{ orbits} &= \frac{1}{|D_3|} \sum_{\sigma \in D_3} |\text{Fix}(\sigma)| = \frac{1}{6}(7^3 + 7 + 7 + 7^2 + 7^2 + 7^2) \\
&= \frac{7}{6}(49 + 1 + 1 + 7 + 7 + 7) = 84
\end{aligned}$$

The question was a little tricky because we are allowed multiple sides to have the same color. A simpler version would restrict to the situation where all sides had to be different colors. In this case D_3 acts on a set of color schemes with cardinality $|Y| = 7 \cdot 6 \cdot 5 = 210$. Moreover, only the identity element has a non-empty fixed set; in this situation the number of distinct toys would be

$$\#\text{ orbits} = \frac{1}{|D_3|} \sum_{\sigma \in D_3} |\text{Fix}(g)| = \frac{1}{6}(210 + 0 + \cdots + 0) = \frac{210}{6} = 35$$

Of course you could answer these questions by pure combinatorics without any resort to group theory!

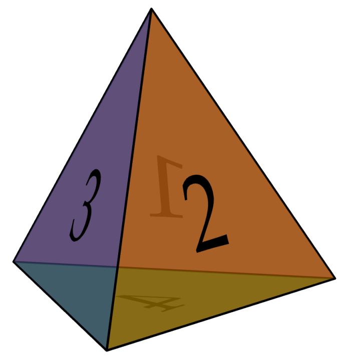
Dice-rolling for Geeks!



Games like Dungeons & Dragons make use of several differently shaped dice: rather than simply using the standard 6-sided cubic die, situations might require rolling, say, a 4-sided tetrahedral die or a 20-sided icosahedral die.

Since dice are designed for rolling, we consider two dice to be the same if one can be rotated into the other. Play with the two tetrahedral dice on the right; you should be convinced that you cannot rotate one to make the other so these dice are distinct.

It is not difficult to see that, up to rotations, these are the *only* tetrahedral dice just by counting!



- Place face 4 on the table.
- When looking from above, the remaining faces are numbered 1, 2, 3 either clockwise or counter-clockwise.

For larger dice, this approach is not practical! However, with a little thinking about symmetry groups, Burnside's formula will ride to the rescue.

Suppose a regular polyhedron has f faces, each with n sides.

- The faces may be labelled 1 thorough f in $f!$ distinct ways: the set of distinct labellings is X.
- We may rotate the polyhedron so that any face is mapped to any other, *in any orientation.* It follows that the rotation group G has fn elements.
- Each non-identity element of the rotation group moves at least one face, whence

$$|\mathrm{Fix}(g)| = \begin{cases} X & \text{if } g = e \\ \emptyset & \text{if } g \neq e \end{cases}$$

- The number of distinct dice for a regular polyhedron is therefore

$$\#\text{ orbits} = \frac{1}{|G|}\,|\mathrm{Fix}(e)| = \frac{|X|}{|G|} = \frac{f!}{fn} = \frac{(f-1)!}{n}$$

  We don't need to know what the rotation group is, only its *order*. For completeness, here are all the possibilities for the regular platonic solids.

Polyhedron	f	n	Rotation Group	# distinct dice
Tetrahedron	4	3	A_4	2
Cube	6	4	S_4	30
Octahedron	8	3	S_4	1,680
Dodecahedron	12	5	A_5	7,983,360
Icosahedron	20	3	A_5	40,548,366,802,944,000

Subgroups of Prime Order & the Class Equation

We finish with a taste of where group theory traditionally goes next.

Suppose G acts on a finite set X, that $x_1 \ldots, x_r$ are representatives of the distinct orbits and that $x_1, \ldots, x_s$ enumerate the 1-element orbits ($\mathrm{Stab}(x_j) = G \iff j \le s$). Then, by counting elements,

$$|X| = s + \sum_{j=s+1}^{r} |Gx_j| = s + \sum_{j=s+1}^{r} \big(G : \mathrm{Stab}(x_j)\big)$$

When G acts on itself by conjugation, the 1-element orbits together comprise the center of G and we obtain the *class equation*:

$$|G| = |Z(G)| + \sum_{j=s+1}^{r} \big(G : \mathrm{Stab}(x_j)\big)$$

Example 8.13. Since the conjugacy classes in S_4 are the cycle types, the class equation reads

$$24 = |\{e\}| + |\text{2-cycles}| + |\text{3-cycles}| + |\text{4-cycles}| + |\text{2,2-cycles}| = 1 + 6 + 8 + 6 + 3$$

Here is an example of how the class equation may be applied.

Lemma 8.14. *Suppose G is a non-abelian group whose order is divisible by a prime p. Then G has a* proper *subgroup whose order is divisible by p.*

Proof. Since G is non-abelian, $Z(G)$ is a proper subgroup. Let x be any element *not* in the center. Then

$$2 \le |Gx| = \frac{|G|}{|\mathrm{Stab}(x)|} \implies \mathrm{Stab}(x) \text{ is a proper subgroup of } G$$

If p divides $|\mathrm{Stab}(x)|$, then we're done. If not, then p divides $|Gx| = \big(G : \mathrm{Stab}(x)\big)$. If this holds for all non-trivial orbits, the class equation says that $|Z(G)|$ is divisible by p. ∎

Theorem 8.15 (Cauchy). *If a prime p divides $|G|$, then G contains a subgroup/element of order p.*

It might feel as if we've done this already; Exercise 4.13 covers abelian groups, but this depends on the fundamental theorem, which first requires Cauchy for abelian groups!

Proof.
1. A proof for when G is abelian is in the exercises.
2. If G is non-abelian, apply the Lemma. If the resulting subgroup is abelian, part 1 finishes things off. Otherwise repeat. If we never reach an abelian subgroup, then we have an infinite sequence of proper subgroups and thus a decreasing sequence of positive integers; contradiction. ∎

Cauchy's Theorem may be extended to prove that if p^k divides G, then G has a subgroup of order p^k. This is the beginning of the Sylow theory of p-subgroups which has applications to group classification and the existence of sequences of normal subgroups.

[26] The two are equivalent: if y has order p, then $\langle y \rangle$ is a subgroup of order p. If $H \le G$ has order p, then $H \cong \mathbb{Z}_p$ is cyclic.

Exercises 8.2. Key concepts:

Orbits of G partition X *Cardinality of orbit* $|Gx| = (G : \mathrm{Stab}(x))$ *divides* $|G|$
Burnside's formula for counting number of orbits

1. Determine the orbits of $G = \langle \sigma \rangle$ on $X = \{1, 2, 3, 4, 5, 6\}$ for each of Exercises 8.1.2 and 3. In both cases verify Burnside's formula.

2. Revisit Example 8.12. How may distinct toys may be created if:

   (a) A maximum of two colors can be used?

   (b) Exactly two colors must be used?

3. Prove Lemma 8.8: the orbits of a left action partition X.

4. A 10-sided die is shaped so that all faces are congruent *kites*: five faces are arranged around the north pole and five around the south, so that each face is adjacent to four others.

   (a) Argue that the group of rotational symmetries of such a die has ten elements. (*In fact it is non-abelian and is therefore isomorphic to* D_5).

   (b) Use Burnside's formula to determine how many distinct 10-sided dice may be produced.

5. A soccer ball is constructed from 20 regular hexagons and 12 regular pentagons as in the picture.
   Suppose the 20 hexagonal patches are all to have different colors, as are the 12 pentagonal patches. How many distinct balls may be produced?

6. The faces of a cuboid measuring $1 \times 1 \times 2$ in is to be painted using (at most) two colors. Up to equivalence by rotations, how many ways can this be done?

7. Repeat the previous question for a regular tetrahedron.

8. Suppose G is a finite group with order p^n where p is a prime. If $x \in G$ lies in a conjugacy class with at least 2 elements, prove that the order of $\mathrm{Stab}(x)$ divides p^{n-1}. Now use the class equation to prove that p divides the order of the center $Z(G)$.

9. We prove the abelian part of Cauchy's Theorem by induction on the order of G.

   (a) Explain why the base case $|G| = 2$ is true.

   (b) Suppose p divides $|G| \geq 3$ and assume the result holds for all abelian groups of order $< |G|$.

   - Choose any $x \neq e$; denote its order by $m = |\langle x \rangle|$ (necessarily $m \geq 2$).
   - Choose a prime q dividing m, define $y := x^{m/q}$ and let $H := \langle y \rangle$.

   Why are we done if $q = p$?

   (c) If $q \neq p$, explain why there exists a coset $zH \in {}^{G}/_{H}$ of order p.

   (d) Prove that z^q has order p in G.