# 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 $\rho_2$ 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

$$\mu_1 \circ \rho_2 = \mu_3$$

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

| $\circ$ | $e$ | $\rho_1$ | $\rho_2$ | $\mu_1$ | $\mu_2$ | $\mu_3$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $\rho_1$ | $\rho_2$ | $\mu_1$ | $\mu_2$ | $\mu_3$ |
| $\rho_1$ | $\rho_1$ | $\rho_2$ | $e$ | $\mu_3$ | $\mu_1$ | $\mu_2$ |
| $\rho_2$ | $\rho_2$ | $e$ | $\rho_1$ | $\mu_2$ | $\mu_3$ | $\mu_1$ |
| $\mu_1$ | $\mu_1$ | $\mu_2$ | $\mu_3$ | $e$ | $\rho_1$ | $\rho_2$ |
| $\mu_2$ | $\mu_2$ | $\mu_3$ | $\mu_1$ | $\rho_2$ | $e$ | $\rho_1$ |
| $\mu_3$ | $\mu_3$ | $\mu_1$ | $\mu_2$ | $\rho_1$ | $\rho_2$ | $e$ |

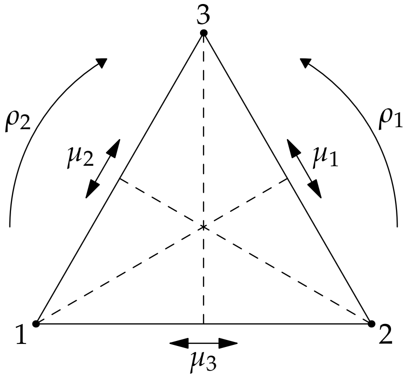
[2] We will return to this notation in Chapter 5, so don't feel you have to be an expert now. The permutation (12) is known as a *2-cycle* because it permutes two objects. The permutation (123) is similarly a *3-cycle.*

**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: $\rho_1$ and $\rho_2$ are rotations, while each $\mu_i$ performs a reflection in the altitude through the $i^{\text{th}}$ 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* $\rho_1, \rho_2$ and the *reflections* $\mu_1, \mu_2, \mu_3$ 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,

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

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,

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

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:

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

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.*

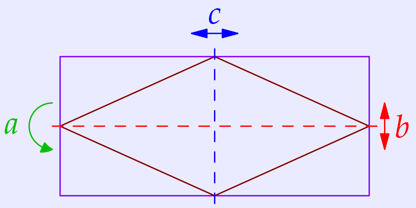
Checking the other axioms is an exercise: the identity is considered a rotation (by 0°!).

**Definition 2.14.** 1. If $\rho_k$ 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) $\mathcal{K} = \{A \in M_2(\mathbb{R}) : \det A = \pm 1\}$   (b) $\mathcal{L} = \{A \in M_2(\mathbb{R}) : \det A = 7\}$

   (c) $\mathcal{N} = \left\{ \left( \begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix} \right) \in M_2(\mathbb{R}) : ad \neq 0 \right\}$

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

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

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

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 $\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) : A^T A = I\}$ 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

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

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°.

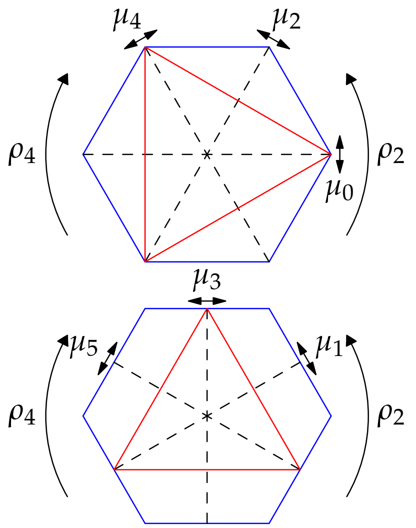
**Geometric subgroup proofs** Arranging figures such that every symmetry of one is also a symmetry of the other immediately results in a subgroup relationship!

**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:

- $\rho_k$ is rotation counter-clockwise by $60k°$; the identity is $\rho_0$.
- The $\mu_k$ 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 $\rho_k$ 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 $\phi$ 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 $\phi$:

- 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 $\phi$ 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 $\phi$ 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!

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

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

### 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 $\phi$ 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 $\phi^{-1}$ 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) $\phi : (M_2(\mathbb{R}), \cdot) \to (\mathbb{R}, \cdot),\ \phi(A) = \det A$

   (h) $\phi : (M_n(\mathbb{R}), +) \to (\mathbb{R}, +)$, $\phi(A) = \operatorname{tr} A =$ 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 $\phi$ 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 $\phi$ 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 $\phi$ 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: $\phi$ 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, $\phi$ 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 $\rho_1$, 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:

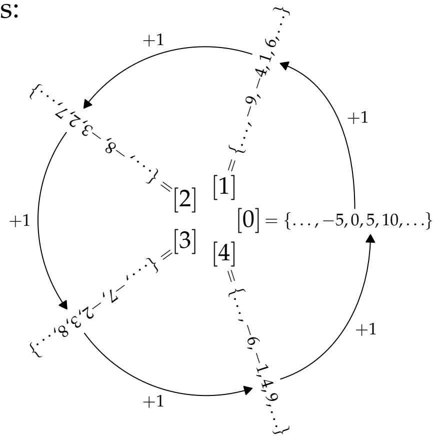
(a) Modular arithmetic: $4 + 2 \equiv 6 \equiv 1 \pmod 5$.

(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!



$+1$
$+1$
$+1$
$+1$
$+1$
$[0] = \{\ldots, -5, 0, 5, 10, \ldots\}$
$[1] = \{\ldots, -9, -4, 1, 6, \ldots\}$
$[2] = \{\ldots, -8, -3, 2, 7, \ldots\}$
$[3] = \{\ldots, -7, -2, 3, 8, \ldots\}$
$[4] = \{\ldots, -6, -1, 4, 9, \ldots\}$

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 $\rho_k \rho_l = \rho_{k+l \,(\mathrm{mod}\ 3)}$

### 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]

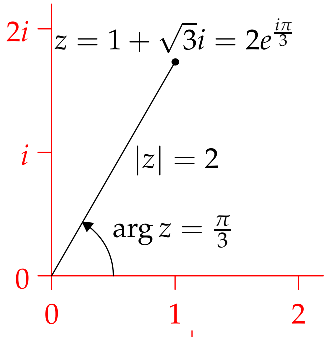
$$e^{i\theta} = \cos\theta + i\sin\theta$$

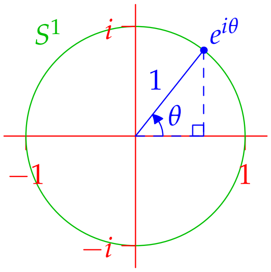
the source of the famous identity $e^{i\pi} = -1$. In the picture, $S^1$ denotes the unit circle. Note also that

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

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!

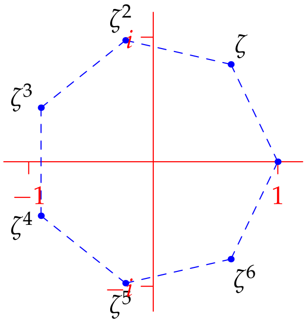
If necessary, write $\zeta_n = e^{\frac{2\pi i}{n}}$ to emphasize $n$.

The square roots of unity are simply ±1, and we saw the 4th roots $\pm 1, \pm i$ in Example 3.1. The $n^{\text{th}}$ 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 $\zeta^{n-1}$, 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!

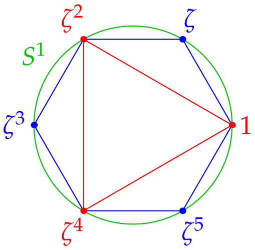
**Lemma 3.10.** *For any $z \in \mathbb{C}$, $\zeta_n^k z = \rho_k(z)$ is the result of rotating $z$ counter-clockwise by $\frac{2\pi k}{n}$ radians.*

**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:

| $\cdot$ | $1$ | $\zeta$ | $\zeta^2$ |
|---|---|---|---|
| $1$ | $1$ | $\zeta$ | $\zeta^2$ |
| $\zeta$ | $\zeta$ | $\zeta^2$ | $1$ |
| $\zeta^2$ | $\zeta^2$ | $1$ | $\zeta$ |

| $\cdot$ | $\zeta^0$ | $\zeta^1$ | $\zeta^2$ |
|---|---|---|---|
| $\zeta^0$ | $\zeta^0$ | $\zeta^1$ | $\zeta^2$ |
| $\zeta^1$ | $\zeta^1$ | $\zeta^2$ | $\zeta^0$ |
| $\zeta^2$ | $\zeta^2$ | $\zeta^0$ | $\zeta^1$ |

| $+_3$ | $0$ | $1$ | $2$ |
|---|---|---|---|
| $0$ | $0$ | $1$ | $2$ |
| $1$ | $1$ | $2$ | $0$ |
| $2$ | $2$ | $0$ | $1$ |

| $\circ$ | $\rho_0$ | $\rho_1$ | $\rho_2$ |
|---|---|---|---|
| $\rho_0$ | $\rho_0$ | $\rho_1$ | $\rho_2$ |
| $\rho_1$ | $\rho_1$ | $\rho_2$ | $\rho_0$ |
| $\rho_2$ | $\rho_2$ | $\rho_0$ | $\rho_1$ |

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 $\rho_1$? Generated by $\mu_1$?
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 $0 \le y \le x \le n-1$, then

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

since $0 \le x - y < n - 1$ 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 7th 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 $\xi = e^{\frac{2\pi i}{\sqrt{2}}}$ and consider the cyclic subgroup $G := \langle \xi \rangle < (\mathbb{C}^\times, \cdot)$. For integers $m$, observe that

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

We conclude that $G$ is an infinite cyclic group and that $\phi : \mathbb{Z} \to G : z \mapsto \xi^z$ is an isomorphism. We can interpret $\xi$ 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 $H \cong G$.*

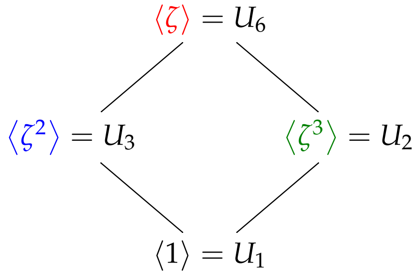
**Example 3.18.** It is helpful to write this out explicitly in additive notation when $G = \mathbb{Z}$. Since every subgroup is cyclic, there are two cases:

- 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.

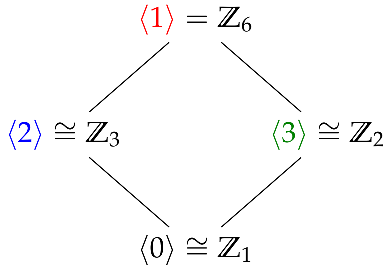
| $x$ | subgroup $\langle x \rangle$ |
|---|---|
| $1$ | $\{1\}$ |
| $\zeta$ | $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ |
| $\zeta^2$ | $\{1, \zeta^2, \zeta^4\}$ |
| $\zeta^3$ | $\{1, \zeta^3\}$ |
| $\zeta^4$ | $\{1, \zeta^4, \zeta^2\}$ |
| $\zeta^5$ | $\{1, \zeta^5, \zeta^4, \zeta^3, \zeta^2,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


$\langle \zeta \rangle = U_6$
$\langle \zeta^2 \rangle = U_3$
$\langle \zeta^3 \rangle = U_2$
$\langle 1 \rangle = U_1$

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


$\langle 1 \rangle = \mathbb{Z}_6$
$\langle 2 \rangle \cong \mathbb{Z}_3$
$\langle 3 \rangle \cong \mathbb{Z}_2$
$\langle 0 \rangle \cong \mathbb{Z}_1$

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 $(\mathbb{Z}_n, +_n)$:

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

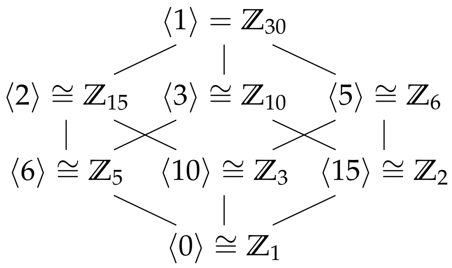
In particular: $x \in \mathbb{Z}_n$ is a generator if and only if $\gcd(x, n) = 1$.

**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.



$\langle 1 \rangle = \mathbb{Z}_{30}$
$\langle 2 \rangle \cong \mathbb{Z}_{15}$
$\langle 3 \rangle \cong \mathbb{Z}_{10}$
$\langle 5 \rangle \cong \mathbb{Z}_6$
$\langle 6 \rangle \cong \mathbb{Z}_5$
$\langle 10 \rangle \cong \mathbb{Z}_3$
$\langle 15 \rangle \cong \mathbb{Z}_2$
$\langle 0 \rangle \cong \mathbb{Z}_1$

**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 $4^{\text{th}}$ 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 $\phi$ 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*

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

*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

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

[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 $A$.

   | $\circ$ | $e$ | $\sigma$ |
   |---|---|---|
   | $e$ | $e$ | $\sigma$ |
   | $\sigma$ | $\sigma$ | $e$ |

   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 $\sigma$ is a bijection, then its inverse function $\sigma^{-1}$ 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 $\tau$ 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

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

$$\begin{tikzcd} a_1 \arrow[r, mapsto] & a_2 \arrow[r, mapsto] & a_3 \arrow[r, mapsto] & \cdots \arrow[r, mapsto] & a_k \arrow[llll, bend right, mapsto] \end{tikzcd}$$

$$\begin{tikzcd} \text{all other } x \arrow[loop right] \end{tikzcd}$$

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 |

$$\begin{tikzcd} \sigma : 1 \arrow[r, mapsto] & 3 \arrow[r, mapsto] & 4 \arrow[r, mapsto] & 2 \arrow[lll, bend right, mapsto] \end{tikzcd}$$

$$\begin{tikzcd} \tau : 1 \arrow[r, bend right] & 4 \arrow[l, bend right] & 2 \arrow[loop right] & 3 \arrow[loop right] \end{tikzcd}$$

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 |

$$\begin{tikzcd} \sigma\tau : 1 \arrow[r, bend right] & 2 \arrow[l, bend right] & 3 \arrow[r, bend right] & 4 \arrow[l, bend right] \end{tikzcd}$$

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: $\sigma\tau = (1$
- Since $1 \overset{\tau}{\mapsto} 4 \overset{\sigma}{\mapsto} 2$, write 2 next: $\sigma\tau = (1\,2$
- $2 \overset{\tau}{\mapsto} 2 \overset{\sigma}{\mapsto} 1$ starts the cycle; close it and open another with an unused value: $\sigma\tau = (1\,2)(3$
- $3 \overset{\tau}{\mapsto} 3 \overset{\sigma}{\mapsto} 4$, so write 4 next: $\sigma\tau = (1\,2)(3\,4$
- $4 \overset{\tau}{\mapsto} 1 \overset{\sigma}{\mapsto} 3$ starts the current cycle, so close it: $\sigma\tau = (1\,2)(3\,4)$
- 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:

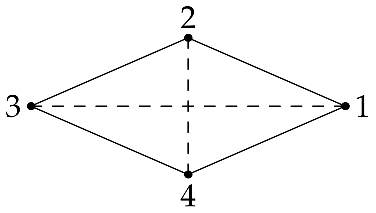
**Examples 5.6.** 1. $(1\,4)(1\,3\,4\,2) = (1\,3)(2\,4)$ 2. $(1\,3\,5\,4)(2\,3\,4) = (1\,3)(2\,5\,4)$

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

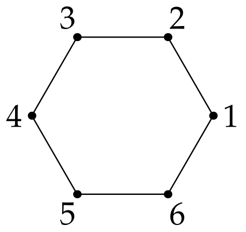
Permutations allow us to describe the group of symmetries of a geometric figure: simply label the vertices (or edges/faces) with numbers $1, 2, 3, \ldots$ and represent each rotation/reflection by how it permutes these values. Cycle notation makes calculating compositions of symmetries easy!

**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°.



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

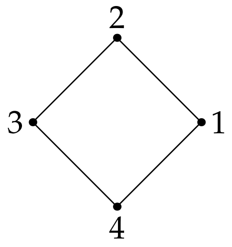
2. Label the vertices of a regular hexagon 1 through 6.



   - 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 ($\delta_j$) and the midpoints of sides ($\mu_j$) differently.



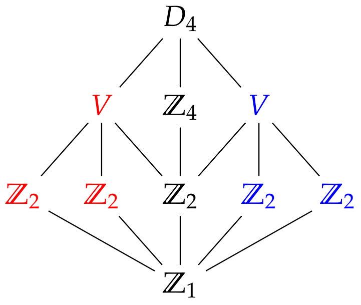
   Cycle notation makes calculation easy: for instance

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

   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 | $\rho_0$ | $e = ()$ |
| | $\rho_1$ | (1234) |
| | $\rho_2$ | (13)(24) |
| | $\rho_3$ | (1432) |
| Reflections | $\mu_1$ | (12)(34) |
| | $\mu_2$ | (14)(23) |
| | $\delta_1$ | (24) |
| | $\delta_2$ | (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 $\sigma_a$ 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 $\sigma_a$ 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 $\sigma_a$ is in the range of $\phi$!

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

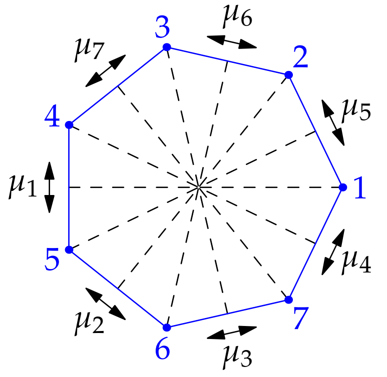
   (d) $(1\,2\,4\,5)^2(2\,4\,5)^2 \in S_5$

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

   (a) State $\mu_4$ 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 $\sigma$ 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*

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

Warning! Each orbit is a subset of $\{1,2,\ldots,n\}$, *not* of the group $S_n$.
Observe also that $\operatorname{orb}_{\sigma^k(x)}(\sigma) = \operatorname{orb}_x(\sigma)$ 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: $\operatorname{orb}_x(\sigma) = \{1,2,3,4\}$ for any $x$. This comports with the result $\sigma = (1\,2\,3\,4)$ of multiplying out $\sigma$ 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 $x \sim y \iff y \in \operatorname{orb}_x(\sigma)$. 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 $\sigma$, 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 $[x] = \operatorname{orb}_x(\sigma)$.

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: $\sigma$ 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

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

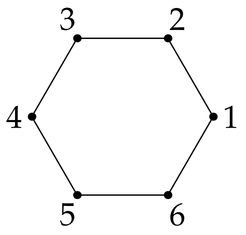
Also, by convention, we delete any orbits of size 1 (1-cycles). If you are still feeling uncomfortable multiplying cycles, practice until it becomes second-nature!

### Orders of Elements in $S_n$

Recall that the order of an element $\sigma$ 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 $\sigma$ is 6. This follows intuitively if we identify $\sigma$ 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 $\sigma^8$. It is *really* tempting to write

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

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 $\sigma$ 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 $\sigma$. 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 $\sigma$ is therefore 6.

**Corollary 5.15.** *The order of a permutation $\sigma$ 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 $\sigma_j^k$ permutes disjoint sets, it follows that

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

If the orbits of $\sigma$ 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 $\alpha_j$ 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 $\sigma^{3465}$, 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: $\text{orb}_a(\sigma) = \{\sigma^j(a) : j \in \mathbb{Z}\}$. 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 $\sigma$.
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 $\sigma^k$ is a subset of an orbit of $\sigma$.
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 $\sigma, \tau, \sigma\tau$ 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 $\sigma$ 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 $\{1, 2, \ldots, n\}$ 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 $\sigma$ 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 $4 \times 4$ 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 $\phi$ is invertible: the inverse of $\phi$ is $\phi$ itself! Moreover, $\phi$ maps even permutations to odd and vice versa. It follows that there are exactly the same number of odd and even permutations. ∎

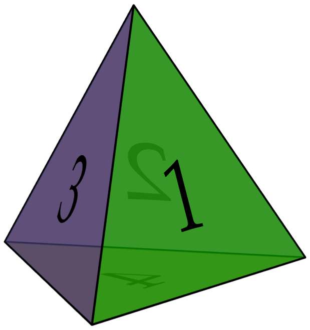
**Examples 5.25.** We describe the small alternating groups up to $A_4$.

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.

$$\begin{aligned} A_4 = \{e, &(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3), \\ &(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \end{aligned}$$

$A_4$ 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 $3 \times 3$ 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 $\rho_1$ odd or even, and how does this depend on $n$?

   (c) Show that every rotation $\rho_i \in D_n$ is generated by $\rho_1$. 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 $\mu$ swap when $n \equiv 1 \pmod 4$? Is $\mu$ 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 $n \not\equiv 1 \pmod 4$.