Math 120A — Introduction to Group Theory

Neil Donaldson

October 5, 2025

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

To *abstract* something means to remove context and application. Modern mathematics largely involves studying patterns and symmetries (often observed in the real world) abstractly so as to observe 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 since Kindergarten!

Example 1.1. The integers $\mathbb{Z} = \{\dots, -1, 0, 1, 2, 3, \dots\}$ together with the operation $+$ form 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] Other 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 In mathematics, the word *group* was first used to describe the ways in which a set could be *reordered*, or *permuted*. 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* (*a translation, rotation* or *reflection*). More general geometries may also be described by their groups of symmetries. Groups may also be employed to describe geometric properties: 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 instance, the set of integers $\mathbb{Z}$ together with the two basic operations of addition and multiplication is a *ring*, as you'll study in a later course.

2 Group Axioms and Basic Examples

In this chapter we define our main objects of study and introduce some of the vocabulary and standard examples used throughout the course. The "Key concepts/definitions" listed at the start of each Exercise set summarize these.

2.1 The Axioms of a Group

Definition 2.1 (Closure). Let G be a set and $*$ a function $* : G \times G \to G$. We describe this arrangement in four different ways, though all mean exactly the same thing:

(a) $\forall x, y \in G,\ x * y \in G$

(b) G is *closed* under $*$.

(c) $*$ is a *binary operation* on G.

(d) $(G, *)$ is a *binary structure.*

In abstract situations (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* $\mathbb{Z}$:

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

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

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 condition (a) is *false,* we 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: $\mathbb{Z}$ is closed under $-$.

3. On a small set, it can be convenient to represent a binary operation in tabular form. The given table describes an operation $*$ on a set of three elements $G = \{e, a, b\}$. Read the *left* column first, then the *top* row: for instance,

$$a * b = e, \text{ or simply } ab = e$$

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

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

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

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

If $*$ is associative, then the expression xyz has unambiguous meaning, as does *exponential* notation: $x^n = x \cdots x$ (n factors).

Examples (2.2, ver. II). 1. Addition is associative: $x + (y + z) = (x + y) + z$ for any integers.

2. $(\mathbb{Z}, -)$ is non-associative: e.g. $(1 - 3) - 2 = -4$, but $1 - (3 - 2) = 0$.

3. $(\{e, a, b\}, *)$, described in the table, is non-associative: e.g. $a(bb) = aa = e$, but $(ab)b = eb = b$.

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

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

Examples (2.2, ver. III). 1. Addition on $\mathbb{Z}$ has identity 0, since $0 + x = x + 0 = x$ for any integer x.

2. $(\mathbb{Z}, -)$ does not have an identity: if $e - x = x$, then $e = -2x$ would depend on x!

3. $(\{e, a, b\}, *)$ has identity e: observe the first row and column of the table.

If G is finite and has an identity (e.g. Example 2.2.3), convention dictates that we list it first. Indeed, we can always list *it* first, since...

Lemma 2.5 (Uniqueness of identity). *A binary structure $(G, *)$ has at most one identity.*

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

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

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

Since $f = e$, there is only one identity. ∎

We used almost nothing about $(G, *)$; in particular it *need not be associative* (e.g. Example 2.2.3).

Definition 2.6 (Inverse). Suppose a binary structure $(G, *)$ has identity e. An element $x \in G$ has an *inverse* $y \in G$ if

$$xy = yx = e$$

Examples (2.2, 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 is irrelevant.

3. Since $ee = aa = ab = ba = e$, we see that every element has an inverse; indeed a has *two* inverses!

Element	e	a	b
Inverses	e	a, b	a

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

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

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

∎

In such a situation it is legitimate to write x^{-1} (or $-x$) for *the* inverse of x. Example 2.2.3 shows that associativity is *necessary*: a non-associative binary 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 (2.2, ver.V). 1. Addition of integers is commutative: $\forall x, y \in \mathbb{Z}$, $x + y = y + x$.

2. Subtraction of integers is *non-commutative*: e.g. $2 - 3 \neq 3 - 2$.

3. The relation is commutative since its table is *symmetric* across the main $\searrow$ diagonal.

To obtain our main definition simply assemble the pieces!

Definition 2.9 (Group axioms). A *group* G 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 a group is the cardinality (size) $|G|$ of the underlying set.[2]
In addition, a group G is said to be *abelian* if the operation $*$ is *commutative.*

In a *multiplicative group*, the operation is written multiplicatively or using juxtaposition (includes composition of functions). A group is *additive*[3] if the operation is addition. Abstract groups are almost always written multiplicatively.

Examples (2.2, ver.VI). 1. $(\mathbb{Z}, +)$ is an *infinite, abelian, additive group*. Precisely the same observations show that $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are also.

2. $(\mathbb{Z}, -)$ is not a group since subtraction is neither associative, nor has an identity (nor inverses).

3. This binary relation is non-associative and so does not define a group.

While it is common practice to refer to a set G as a group, you should do so *only if the operation $*$ is obvious to everyone*. Writing "$\mathbb{Z}$ is a group *under addition*," is safer than "$\mathbb{Z}$ is a group:" it might be a group under many different operations!

Examples 2.10. 1. The non-zero real numbers $\mathbb{R}^\times$ form 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	$1 \in \mathbb{R}^\times$ is the identity since, for any $x \neq 0$, we have $1 \cdot x = x \cdot 1 = x$
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 $xy = yx$

As with addition of integers, we cannot prove these claims since they are part of the definition of multiplication. Similarly, $(\mathbb{Q}^\times, \cdot)$ and $(\mathbb{C}^\times, \cdot)$ are abelian groups.

[2] A *finite group* has finite order, while an *infinite group* has infinite order; unless absolutely necessary, it is rare to be specific about infinite cardinalities (countable, uncountable, etc.).

[3] These are distinctions only of notation. For instance $x + x + x = 3x$ in an additive group corresponds to $xxx = x^3$ in a multiplicative group.

2. The set of *even* integers $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$ forms an abelian group under addition.

3. The set of *odd* integers $1 + 2\mathbb{Z} = \{1 + 2n : n \in \mathbb{Z}\}$ does 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. A *Cayley table*[4] is a tabular representation of a (small) group. Groups of orders 1, 2 and 3 are shown. The one-element group $\{e\}$ is often called the *trivial group*.
   Note the *magic square (sudoku) property*: each row/column contains every element exactly once (see Exercise 11).

$*$	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

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

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

Part 3 should remind you of *matrix multiplication.*

Proof. Parts 1 & 2 are exercises. For part 3, multiply out using associativity:

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

Similarly $(xy)(y^{-1}x^{-1}) = e$. Thus $y^{-1}x^{-1}$ is the inverse of xy (unique by Lemma 2.7). ∎

Exercises 2.1. Key concepts/definitions/examples: make sure you can state the formal definitions.
Group (closure, associativity, identity, inverse) *Commutativity/abelian* *Cayley table*

1. Given the binary operation table, calculate

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

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

2. The table for a binary operation on the set $\{a, b, c\}$ is given. Compute $a * (b * c)$ and $(a * b) * c$. Does the expression $a * b * c$ make sense? 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 (*without writing 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?*)

[4] Englishman Arthur Cayley (1821–95) was an early group theorist. Similarly *abelian* honors the Norwegian Niels Abel (1802–29), after whom the Abel Prize is named (often considered the Nobel Prize in Mathematics).

5. Which are binary structures? For those that are, which are commutative and which associative? Give brief arguments in each case.

   (a) $(\mathbb{Z}, *)$, $a * b = a + b + 1$ (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. Verify the axioms of an abelian group; if any are false, provide a counter-example.

   (a) $\mathbb{N}$ 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. (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 G, we can unambiguously write $(x^{-1})^n = \underbrace{x^{-1} \cdots x^{-1}}_{n \text{ times}}$.

   For any $n \in \mathbb{N}$ and $x \in G$, *prove* that $(x^{-1})^n = (x^n)^{-1}$. By convention, this object is denoted x^{-n}. How would we write this in an *additive* group (Footnote 3)?

8. Let G be a group. Prove:

   (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 $\iff \forall x, y \in G$, $(xy)^{-1} = x^{-1}y^{-1}$

9. Prove or disprove: $(\mathbb{R} \setminus \{1\}, *)$ is an abelian group, where $x * y := x + y - xy$.

10. Let $\mathcal{U}$ be a set and $\mathcal{P}(\mathcal{U})$ its power set (the set of subsets of X).

    (a) Which of the group axioms are 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 $(\mathcal{P}(\mathcal{U}), \triangle)$ a group? Explain your answer.

11. (Magic Square) Suppose $(G, *)$ is associative and that 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

The prefix *sub-* in mathematics usually indicates a *subset* that retains the indicated structure.

Definition 2.12 (Subgroup). Let G be a group. A *subgroup* of G is a non-empty subset $H \subseteq G$ which remains 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* of G is the 1-element set $\{e\}$; all other subgroups are *non-trivial*.

Examples 2.13. The following should be immediate from the definition: all you need is a non-empty subset that remains a group!

1. $\{e\} \leq G$ and $G \leq G$ for *any* group 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. $(2\mathbb{Z}, +) < (\mathbb{Z}, +)$
4. $(\mathbb{R}^m, +) \leq (\mathbb{R}^n, +)$ if $m \leq n$. For instance, with respect to the standard basis, $\mathbb{R}^m$ consists of all column vectors in $\mathbb{R}^n$ whose last $n - m$ entries are zero.
5. $(C(\mathbb{R}), +) < (C^1(\mathbb{R}), +)$. Think back to calculus: the sub of any two continuous functions is continuous; every differentiable function is continuous; etc., etc.

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

Theorem 2.14 (Subgroup criterion). *Let G be a group. A non-empty subset $H \subseteq G$ is a subgroup if and only if it is* closed *and has* inverses *in H (with respect to the group operation on G):*

$$\forall h, k \in H, \;\; hk \in H \text{ and } h^{-1} \in H \qquad (*)$$

Proof. ($\Rightarrow$) H is a group and therefore satisfies all the axioms, including closure and inverse.

($\Leftarrow$) By assumption, H satisfies the *closure* axiom. Moreover, the group operation on G is automatically *associative* on any subset,[5] including H. It remains to verify that the *identity* element e (of G) lies in H, for then our assumption ($h^{-1} \in H$) says that that *inverse* axiom is also satisfied.

Since $H \neq \emptyset$, we may choose some (any!) $h \in H$. By $(*)$, $h^{-1} \in H$. A second application of $(*)$ finishes things off:

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

■

Examples 2.15. 1. All of Examples 2.13 can be confirmed using the theorem. For instance, part 5:

Non-empty subset: plainly $2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\} = \{2z : z \in \mathbb{Z}\}$ is such (of $\mathbb{Z}$).
Closure: $2m, 2n \in 2\mathbb{Z} \implies 2m + 2n = 2(m + n) \in 2\mathbb{Z}$.
Inverses: $2m \in 2\mathbb{Z}$ has inverse $-(2m) = 2(-m) \in 2\mathbb{Z}$.

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

[5] Associativity does not care where $x(yz) = (xy)z$ lives: "$\in G$" does not appear in Definition 2.3!

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

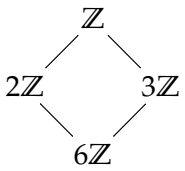
$$1+3\mathbb{Z} = \{1+3n : n \in \mathbb{Z}\} = \{1, 4, 7, 10, 13, \ldots, -2, -5, -8, \ldots\}$$

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 $(\mathbb{Z}, +)$.

4. The *circle group* $S^1 := \{e^{i\theta} : \theta \in [0, 2\pi)\}$ is plainly a non-empty subset of $(\mathbb{C}^\times, \cdot)$. The standard *exponential laws* and the fact that $e^{2\pi i} = 1$ verify that S^1 is in fact a *subgroup*.

Closure: $e^{i\theta}e^{i\psi} = e^{i(\theta+\psi)} \in S^1$ (equals $e^{(\theta+\psi-2\pi)i}$ if you feel it necessary).
Inverses: $(e^{i\theta})^{-1} = e^{-i\theta} = e^{(2\pi-\theta)i}$.

Subgroup Diagrams It can be helpful to represent subgroup relations pictorially, using descending lines. For instance, the diagram on the right summarizes the subgroup relations



$$6\mathbb{Z} < 2\mathbb{Z} < \mathbb{Z}, \qquad 6\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z}, \qquad 6\mathbb{Z} < \mathbb{Z}$$

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

Exercises 2.2. Key concepts: *(Proper/trivial/non-trivial) Subgroup*
Subgroup criterion (non-empty subset, closure, inverses) *Subgroup diagram*

1. Use the subgroup criterion 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. Describe/explain the relationship between positive integers m and n if $(m\mathbb{Z}, +) \leq (n\mathbb{Z}, +)$.
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. Briefly explain why "subgroup" is transitive: that is, if $K \leq H$ and $H \leq G$, then $K \leq G$.
6. Suppose H and K are subgroups of G. Prove that $H \cap K$ is also a subgroup of G.
7. Let H be a non-empty subset of a group G. Prove that H is a subgroup of G if and only if

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

8. (Hard) On an abstract set $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ of eight elements, we define an operation ('multiplication') using several properties:
   - 1 is the identity.
   - -1 commutes with everything in the expected way: e.g. $-i = (-1)i = i(-1)$, etc.
   - $(-1)^2 = 1$, $\quad i^2 = j^2 = k^2 = -1$ and $ij = k$.
   - Multiplication is associative.

   (a) Prove that $(Q_8, \cdot)$ is a non-abelian group by completing its Cayley table.
   (*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 Modular Arithmetic

Many commonly encountered examples in abstract algebra make use of *modular arithmetic*: the addition and multiplication of *remainders*. Such arithmetic should be at least somewhat familiar so we offer only a brief refresher. At present, these groups are very informal and are introduced primarily to supply examples; more rigorous discussions will be given in Chapters 3 & 5.

Definition 2.16. Let n be a positive integer. We denote by $\mathbb{Z}_n$ the set of *equivalence classes of integers modulo n.* These are typically written as remainders (i.e., as integers),

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

where $x = y \in \mathbb{Z}_n$ means that the integers x, y have the *same remainder* on division by n.

More formally,[6] $x = y \in \mathbb{Z}_n$ means $x \equiv y \pmod{n}$, or equivalently $x = y + \lambda n$ for some integer λ.

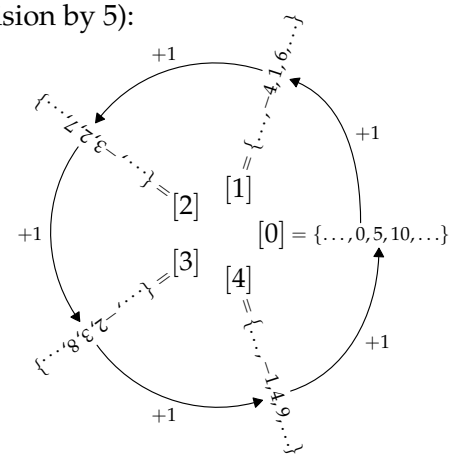
Example 2.17. In the most commonly used notation, we write $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Several other notations are available. For instance, here is a calculation written in four different ways (note that $6 = 1$ in $\mathbb{Z}_5$ because they both have the same remainder 1 on division by 5):

(a) Group/Number Theory style: $4 + 2 = 6 = 1$ in $\mathbb{Z}_5$.

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

(c) Decorated operation: $4 +_5 2 = 6 = 1$.

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



For reasons of brevity we mostly use notation (a), though feel free to use another if it makes you more comfortable. Regardless of notation, you *must* make it clear in *which* $\mathbb{Z}_n$ you are working: $4 + 2 = 1$ is not acceptable on its own!

Theorem 2.18. *$\mathbb{Z}_n$ forms an abelian group of order n under addition modulo n.*

A rigorous proof (in the language of Footnote 6) is tedious, but will come for free in Chapter 5 when $\mathbb{Z}_n$ is properly defined as a *factor group*. These groups are so common that we usually just state "The group $\mathbb{Z}_n$," rather than $(\mathbb{Z}_n, +_n)$. In the exercises, we'll also consider how *multiplication* modulo n can be used to create groups of remainders.

[6] An element of $\mathbb{Z}_n$ is strictly an *equivalence class*: for instance, $[x] \in \mathbb{Z}_n$ denotes the class of all integers with the same remainder as the representative $x \in \mathbb{Z}$:

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

Addition of equivalence classes is *well-defined* (multiplication similarly): if $[x] = [w]$ and $[y] = [z]$, then $w = x + \kappa n$ and $z = y + \lambda n$, from which

$$[w] +_n [z] = [w + z] = \big[(x + \kappa n) + (y + \lambda n)\big] = \big[x + y + n(\kappa + \lambda)\big] = [x + y] = [x] +_n [y]$$

While it is important to appreciate that the elements of $\mathbb{Z}_n$ are not really numbers, the tediousness of this formal language means that it is usually avoided. Equivalence classes and well-definition are not critical right now, but will become so later.

Examples 2.19. Here are the Cayley tables for $\mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3$ and $\mathbb{Z}_4$.

$+_1$	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

In each case 0 is the identity element. If you compare these to the the tables in Example 2.10.6, the patterns should look familiar (we will explore this further in Section 2.5).

Subgroups of $\mathbb{Z}_n$

It is easy to spot certain subgroups of $\mathbb{Z}_n$ — just think about divisors of n!

Example 2.20. Plainly 2 is a divisor of 4. By covering up the rows/columns corresponding to 1 and 3, we obtain the Cayley table for the subgroup $H = \{0, 2\}$ of $\mathbb{Z}_4$.

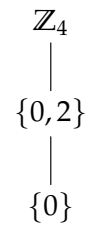
$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\longrightarrow$

$+_4$	0	2
0	0	2
2	2	0

Hopefully it is obvious why H is a subgroup (think about the subgroup criterion Theorem 2.14!). Now suppose 1 were in some subgroup $K \leq \mathbb{Z}_4$ and consider what the group axioms tell us:

$$\left.\begin{array}{ll} \text{Closure} & \Longrightarrow 2 = 1 + 1 \in K \\ \text{Inverse} & \Longrightarrow 3 = -1 \in K \\ \text{Identity} & \Longrightarrow 0 \in K \end{array}\right\} \Longrightarrow K = \{0, 1, 2, 3\} = \mathbb{Z}_4$$



The same thing happens if a subgroup contains 3. The upshot is that $\mathbb{Z}_4$ has precisely three subgroups: itself, $\{0, 2\}$ and the trivial subgroup $\{0\}$. The full subgroup diagram is drawn.

Here is a more general version. Suppose d is a divisor of n, write $n = dk$, and consider the subset of *multiples of* d in $\mathbb{Z}_n$:

$$\langle d \rangle = \{0, d, 2d, \ldots, (k-1)d\}$$

In the language of the subgroup criterion (Theorem 2.14), this set is:

Non-empty: Plainly $0 \in \langle d \rangle$.

Closed under addition: $\kappa d + \lambda d = (\kappa + \lambda)d \in \langle d \rangle$.

Closed under inverses: The inverse of λd is $-\lambda d = (k - \lambda)d \in \langle d \rangle$.

We have therefore proved:

Lemma 2.21. *If d is a divisor of n, then the set of multiples $\langle d \rangle$ in $\mathbb{Z}_n$ is a subgroup of order $\frac{n}{d}$.*

As in Example 2.20, in Chapter 3 we'll see that these are in fact the *only* subgroups of $\mathbb{Z}_n$.

Exercises 2.3. Key concepts: $\mathbb{Z}_n$, *Multiples as subgroups:* $d \mid n \Longrightarrow \langle d \rangle \leq \mathbb{Z}_n$

1. Refresh your memory of modular arithmetic by evaluating the following:

   (a) $17 + 22$ in $\mathbb{Z}_{30}$
   (b) $31 \cdot 4$ in $\mathbb{Z}_{12}$
   (c) 5^6 in $\mathbb{Z}_{14}$,
   (d) $19^2 - 42 \cdot 13$ in $\mathbb{Z}_{17}$

2. State the Cayley tables for the groups $\mathbb{Z}_5$ and $\mathbb{Z}_6$ (more formally $(\mathbb{Z}_5, +_5)$ and $(\mathbb{Z}_6, +_6)$).

3. State the Cayley tables for all proper subgroups of $\mathbb{Z}_6$. Now draw the full subgroup diagram for $\mathbb{Z}_6$.

   (*Hint: consider Lemma 2.21 and the remark that follows*)

4. Draw the subgroup diagram for $\mathbb{Z}_{12}$.

5. Suppose n is a positive integer ≥ 2.

   (a) Explain why $\mathbb{Z}_n$ is *not* a group under *multiplication.* If you're unsure what to do, consider an example: what is the multiplication table for $(\mathbb{Z}_3, \cdot)$?
   (b) Explain why $\{1, 2, 3, 4, 5\}$ isn't a group under multiplication modulo 6.
   (c) Hypothesize for which integers $n \geq 2$ the set $\{1, 2, 3, \ldots, n-1\}$ forms a group under multiplication modulo n. If you want a challenge, try to prove your assertion.

6. The set $\mathbb{Z}_n^\times$ denotes the *units* in $\mathbb{Z}_n$, those elements which are relatively prime to n:

   $$\mathbb{Z}_n^\times = \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}$$

   In part (d), we verify that $\mathbb{Z}_n^\times$ is an abelian group under multiplication modulo n.

   (a) Construct the Cayley tables for the groups $\mathbb{Z}_3^\times = \{1, 2\}$ and $\mathbb{Z}_4^\times = \{1, 3\}$.
   (b) Construct the Cayley table for the group $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$. Now identify its *subgroups.*
   (c) Construct the Cayley tables for $\mathbb{Z}_8^\times$ and $\mathbb{Z}_9^\times$. What is the order of each group?
   (d) (Hard) Prove that $\mathbb{Z}_n^\times$ forms an abelian group under multiplication modulo n by verifying the group axioms.
   (*Hint: Recall Bézout's identity* $\gcd(x, n) = 1 \Longleftrightarrow \exists \kappa, \lambda \in \mathbb{Z}$ *such that* $\kappa x + \lambda n = 1$)
   (e) i. Compare the orders of the groups $\mathbb{Z}_3^\times$, $\mathbb{Z}_4^\times$ and $\mathbb{Z}_{12}^\times$. What do you observe?
   ii. What about the orders of $\mathbb{Z}_2^\times$, $\mathbb{Z}_6^\times$ and $\mathbb{Z}_{12}^\times$? What is going on?
   iii. The order of $\mathbb{Z}_n^\times$ is the value of *Euler's totient function* $\phi(n)$. Research some of the properties of this function: can you find something that helps explain your observations in parts i and ii? Better still, take a course in Number Theory!

2.4 Geometric Symmetries & Matrix Groups

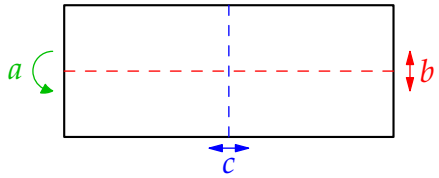
Geometric symmetries an matrices provide further large families of groups.
Now consider any geometric figure that has some symmetry (typically viewed as rotational or reflective), such as a triangle, square, or tetrahedron. Each symmetry corresponds to a *function* that transforms the original figure in such a way that the result occupies the same location as the original.

Example 2.22 (Klein four-group). The pictured rectangle has three obvious symmetries:

(a) Rotation by 180°.

(b) Vertical reflection.

(c) Horizontal reflection.

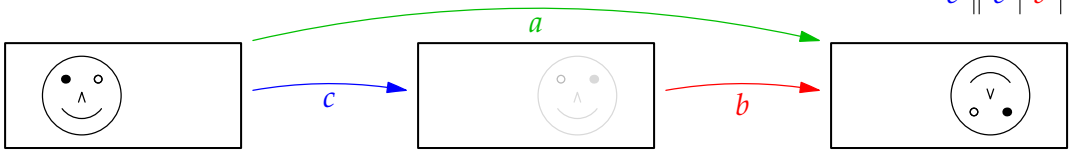


Each symmetry may be viewed as a function transforming the rectangle (or permuting its vertices/edges if you prefer). Group Theorists also consider the *identity function* e as a symmetry: it simply leaves the rectangle alone.[7]

It should be clear that the set $V := \{e, a, b, c\}$ comprises every symmetry of the rectangle. We claim that V forms a group whose binary operation is *composition of functions*.

Closure After applying any two symmetries in sequence, the rectangle still occupies the same location on the page, the result of applying a *single* symmetry. The composition table is shown and is easily be verified by, for instance, drawing a smiley face on one side of a sheet of paper.

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



The pictures confirm $b \circ c = a$: remember that the **right side comes first** when composing functions! The diagonal symmetry of the table shows that the operation is *commutative*.

Associativity Composition of functions is always associative (Exercise 9).

Identity The function e leaves the rectangle alone. Plainly $e \circ f = f \circ e = f$ for any symmetry f.

Inverse To find the inverse of a symmetry, simply undo what you just did! In the case of the rectangle, every symmetry is its own inverse.

The symmetries of the rectangle thus form an abelian group of order 4. This is named the *Klein four-group* in honor of Felix Klein, a 19th century German mathematician whose application of group theory transformed modern geometry. The letter V comes from the original German: *vierergruppe.*

[7] There is little benefit to being explicit, but if you choose co-ordinates with the origin at the center of the rectangle, these functions can be written formulaically:

$$e(x,y) = (x,y), \qquad a(x,y) = (-x,-y), \qquad b(x,y) = (x,-y), \qquad c(x,y) = (-x,y)$$

A similar discussion applies to any geometric figure.

Theorem 2.23. *The* symmetries *of any geometric figure form a group under composition. The* orientation-preserving symmetries *form a subgroup, often called the* rotation group.[8]

Example (2.15.4, cont.). Since the complex function $z \mapsto e^{i\theta}z$ *rotates* counter-clockwise by θ around the origin, the *circle group* S^1 may be viewed as the group of rotations of the plane (or the circle).

Definition 2.24. A regular n-gon has two commonly associated symmetry groups.

Dihedral Group The full symmetry group D_n has order $2n$. It splits into two subsets of size n:

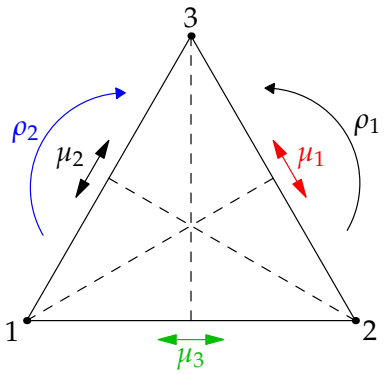
Rotations Labelled $e, \rho_1, \ldots, \rho_{n-1}$ where ρ_k rotates counter-clockwise by $\frac{2\pi k}{n}$ radians ($\frac{360k}{n}°$). The identity $e = \rho_0$ is considered a rotation (by 0°).

Reflections These are typically labelled μ_k or δ_k.

Rotation group Denoted $R_n = \{e, \rho_1, \ldots, \rho_{n-1}\}$. This group is *abelian*, which follows because composition of rotations simply sums angles:

$$\rho_j \circ \rho_k = \rho_{j+k \pmod n} = \rho_{k+j \pmod n} = \rho_k \circ \rho_j$$

Example 2.25. Denote the elements of the dihedral group D_3 as in the picture, where labeling the vertices 1, 2, 3 helps to keep track of things:



$$D_3 = \{e, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$$

Its Cayley table is below. Constructing the table from scratch is a lot of work and is not worth memorizing!

The highlighted computation is $\mu_1 \circ \rho_2 = \mu_3$ (remember to 'do' ρ_2 to the triangle first!). To verify, we could again try the smiley face trick, or alternatively consider the movement of a vertex:

> ρ_2 moves vertex 1 to vertex 3; μ_1 moves this to vertex 2. Since the composition of a rotation and a reflection is a reflection (the triangle has been flipped over once!), the result must be the reflection mapping $1 \mapsto 2$, namely μ_3.

The lack of symmetry in the Cayley table shows that D_3 is a *non-abelian group*: indeed

$$\rho_2 \circ \mu_1 = \mu_2 \neq \mu_3 = \mu_1 \circ \rho_2$$

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

The Cayley table for the (abelian) rotation group $R_3 = \{e, \rho_1, \rho_2\}$ is visible in the top left corner.

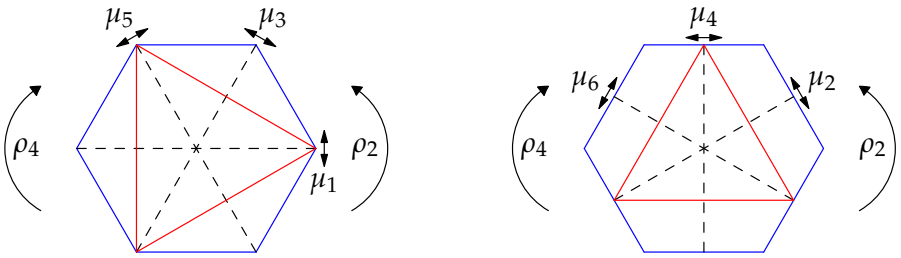
[8] In low dimensions, *orientation-preserving* means that a transformation doesn't change the usual *right-hand rule* (e.g., cross products). In two dimensions these are precisely the *planar rotations*. In three dimensions a general orientation-preserving symmetry is the composition of two pure rotations (recall spherical polar co-ordinates).

Geometric Subgroup Relations

These are often straightforward to observe by drawing two shapes in such a way that all the symmetries of one are also symmetries of the other. Since the symmetries of both shapes form a group, this pictorial approach justifies the only necessary condition in Definition 2.12: the subset property.

Examples 2.26. 1. For any n, we see that $R_n < S^1$: every rotation of a regular n-gon is also a rotation of a circle (with the same center).

2. Consider a regular hexagon, inside which have been drawn two equilateral triangles. Every symmetry of either triangle is also a symmetry the hexagon. We conclude:



(a) $R_3 < R_6$. Be careful with notation! With respect to the hexagon, ρ_k is rotation counterclockwise by $60k°$, whence the subgroup relation should be written

$$R_3 = \{e, \rho_2, \rho_4\} < R_6 = \{e, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$$

Also note that *both triangles have the same rotation group.*

(b) $D_3 < D_6$. This is a little more complicated. Labeling the reflections $\mu_1, \ldots, \mu_6$ as in the picture, we see that the two triangles actually have different (full) symmetry groups:

$$D_3^I = \{e, \rho_2, \rho_4, \mu_1, \mu_3, \mu_5\} < D_6 \quad \text{and} \quad D_3^{II} = \{e, \rho_2, \rho_4, \mu_2, \mu_4, \mu_6\} < D_6$$

Otherwise said, D_6 has two *distinct* subgroups that look like D_3.

Matrix Groups

As observed in any elementary linear algebra course (see also Exercise 10), **matrix multiplication is associative**. This quickly yields several examples.

Example 2.27. The *general linear group* comprises the invertible $n \times n$ matrices under multiplication. For this course, only such matrices with real number entries will be encountered:

$$\mathrm{GL}_n(\mathbb{R}) = \left\{A \in \mathrm{M}_n(\mathbb{R}) : \det A \neq 0\right\} \qquad \text{(non-abelian when } n \geq 2\text{)}$$

Since **associativity** holds in general, we need only verify the other three axioms.

Closure follows from the familiar result $\det AB = \det A \det B$.

The **identity** (drum roll…) is the *identity matrix* I.

$$I = \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & \ddots & \\ & \ddots & \ddots & 0 \\ & & 0 & 1 \end{pmatrix}$$

Finally, **invertibility** is assumed. Part 3 of Theorem 2.11 should now seem very familiar: $(xy)^{-1} = y^{-1}x^{-1}$.

Matrix subgroups

The general linear group $\mathrm{GL}_n(\mathbb{R})$ has many subgroups. Here is one; some others are in the Exercises.

Example 2.28. The *orthogonal group* $\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) : A^T A = I\}$ consists of those matrices whose inverse equals their transpose ($A^{-1} = A^T$). We verify that this is a subgroup of $\mathrm{GL}_n(\mathbb{R})$ using the subgroup criterion (Theorem 2.14) and simple matrix properties.

Non-empty subset Every orthogonal matrix is invertible, whence $\mathrm{O}_n(\mathbb{R}) \subseteq \mathrm{GL}_n(\mathbb{R})$. This is immediate in two ways: if $A \in \mathrm{O}_n(\mathbb{R})$, then,

$$A^T A = I \implies A^{-1} = A^T \text{ exists, or,}$$
$$1 = \det I = \det A \det A^T = (\det A)^2 \implies \det A \neq 0$$

Moreover, $I^T I = I^2 = I$, so $I \in \mathrm{O}_n(\mathbb{R})$: we have non-emptiness.

Closure Suppose $A, B \in \mathrm{O}_n(\mathbb{R})$. Then

$$(AB)^T(AB) = B^T A^T AB = B^T IB = B^T B = I \implies AB \in \mathrm{O}_n(\mathbb{R})$$

Inverses Suppose $A \in \mathrm{O}_n(\mathbb{R})$. Then

$$(A^{-1})^T A^{-1} = (A^T)^T A^T = (AA^T)^T = I^T = I \implies A^{-1} \in \mathrm{O}_n(\mathbb{R})$$

The 2×2 orthogonal matrices can be interpreted as rotations and reflections.[9] For instance, the matrix $\frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & -1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{O}_2(\mathbb{R})$ rotates the plane counter-clockwise by 45°.

Exercises 2.4. Key concepts: *Klein 4-group* V *Dihedral group* D_n *Rotation group* R_n *Geometric subgroup relations* *General linear group* $\mathrm{GL}_n(\mathbb{R})$

1. Use Theorem 2.14 to explain why the set of *rotations* of a planar figure is a subgroup of its full symmetry group (rotations *and* reflections).
2. Explicitly state the Cayley table for the rotation group R_4 of a square.
3. Find the subgroup diagram of the Klein four-group. Explain how you know you are correct.
4. Repeat the previous question for the rotation group R_6.
5. (a) Find all subgroups and the subgroup diagram for the group D_3.
   (Don't worry about being rigorous as to how you know you've found them all.)
   (b) Describe the symmetry group and Cayley table of a *non-equilateral* isosceles triangle. What about a *scalene* triangle?

[9] You might have seen this in another course. Left-multiplication by:

- $\left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right)$ rotates vectors counter-clockwise by θ radians.
- $\left(\begin{smallmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{smallmatrix}\right)$ reflects across the line making angle $\theta/2$ with the positive real axis.

This interpretation allows us to view D_n as a subgroup of $\mathrm{O}_2(\mathbb{R})$.

6. (a) Represent the elements of the Klein four-group V (as in Footnote 7) using matrix notation (i.e. a is left-multiplication by what matrix). As such, identify V as a subgroup of $\mathrm{O}_2(\mathbb{R})$.
   (b) Modeling Example 2.26, draw three pictures which describe different ways in which V may be viewed as a subgroup of D_6.

7. Determine whether each of the following sets of matrices is a group under multiplication.
   (a) $\mathcal{K} = \{A \in \mathrm{M}_2(\mathbb{R}) : \det A = \pm 1\}$ (b) $\mathcal{L} = \{A \in \mathrm{M}_2(\mathbb{R}) : \det A = 7\}$
   (c) $\mathcal{N} = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{R}) : ad \neq 0 \right\}$

8. Prove that each set of matrices forms a group under multiplication (don't memorize these—unless you really love matrices...).
   (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) (Hard) $\mathrm{SL}_n(\mathbb{Z}) = \{A \in \mathrm{M}_n(\mathbb{Z}) : \det A = 1\}$: 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

   $$\mathrm{GL}_n(\mathbb{R}), \quad \mathrm{SL}_n(\mathbb{R}), \quad \mathrm{O}_n(\mathbb{R}), \quad \mathrm{SO}_n(\mathbb{R}), \quad \mathcal{Q}_n, \quad \mathrm{SL}_n(\mathbb{Z})$$

9. (a) Let X be any set. Prove that composition of functions $f : X \to X$ is associative. (*Hint:* $(f \circ g) \circ h = f \circ (g \circ h)$ *means that both functions do the same thing to the same input...*)
   (b) Suppose X contains at least two distinct elements $a \neq b$. Prove that there exist functions $f, g : X \to X$ for which $f \circ g \neq g \circ f$.

10. (a) Prove that matrix multiplication of (real square) matrices is associative. (*Hint: If A has entries (a_{ij}), etc., what are the pq^{th} entries of the matrices $A(BC)$ and $(AB)C$?*)
    (b) Show that multiplication of (invertible) $n \times n$ matrices is non-commutative when $n \geq 2$.

11. Prove that D_n is non-abelian ($n \geq 3$).
    (*Hint: label vertices and proceed as is Example 2.25*)

12. Consider rotating (in 3D) a regular tetrahedron. Any face (equilateral triangle) may be rotated to its desired location (four options), in which it has three possible orientations. The rotation group of the tetrahedron therefore has $4 \times 3 = 12$ elements.
    (a) Find the order of the rotation group of a cube.
    (b) Repeat for a regular octahedron. Give a *geometric* reason why your answer is the same as part (a).
    (*Hint: Try joining the midpoints of each face...*).
    (c) What about the dodecahedron and the icosahedron?!


Common polyhedral dice

In case you don't recognize it, the pictured red die is not one of the five Platonic solids: it has ten rhombus-shaped faces, and its rotation group has order 10. We'll return to these examples in later sections.

2.5 Homomorphisms & Isomorphisms

In the previous sections, you should have felt like you were encountering similar examples in different contexts. A key goal of abstract mathematics is the comparison of similar/identical structures with outwardly different appearances. The standard approach to such comparison is uses *functions*.

Example 2.29. Compare the rotation group R_3 of an equilateral triangle to the modular arithmetic group $\mathbb{Z}_3$. Their Cayley tables look almost identical, particularly if we write ρ_0 for the identity in R_3. To a mathematician, the groups have the same *structure*; they are merely labelled differently.

Relabelling means defining an *invertible function* $\mu : R_3 \to \mathbb{Z}_3$: the obvious choice from looking at the tables is $\mu(\rho_k) = k$.

Since the tables describe all possible interactions between the elements of each group, it is clear that μ satisfies

$$\forall \rho_j, \rho_k \in R_3, \;\; \mu(\rho_j \circ \rho_k) = \mu(\rho_j) +_3 \mu(\rho_k)$$

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

$(R_3, \circ)$

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

$(\mathbb{Z}_3, +_3)$

Indeed, both sides simply equal $j +_3 k$! This is a critical formula. To see why, suppose we are given remainders $x, y \in \mathbb{Z}_3$ and consider two courses of action:

1. *First combine* the remainders $x +_3 y$ in $\mathbb{Z}_3$, *then map* to R_3 using the function to obtain $\mu(x +_3 y)$.
2. *First map* both remainders to R_3 using μ, *then combine* in R_3 to obtain $\mu(x) \circ \mu(y)$.

Regardless of the order (combine/map or map/combine) *we always obtain the same result*! Such *structure-preserving functions* are at the heart of abstract algebra.

Definition 2.30 (Homo- & Isomorphisms). Suppose $(G, *)$ and $(H, \star)$ are binary structures and $\phi : G \to H$ a function. We say that ϕ is a *homomorphism* of binary structures if

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

An *isomorphism*[10] of binary structures G, H is a *bijective/invertible homomorphism* $\mu : G \to H$.

Binary structures G, H are *isomorphic*, written $G \cong H$, if there exists some isomorphism $\mu : G \to H$.

The notation is typical: μ (rather than ϕ) is often used when we know we have an *iso*morphism. For most of these notes (certainly after this chapter), all binary structures will be groups.

Examples 2.31. 1. (2.29 cont.) We have *isomorphic groups* $R_3 \cong \mathbb{Z}_3$. Indeed the function $\mu : R_3 \to \mathbb{Z}_3$ is an *isomorphism of groups* (or *group isomorphism*).

2. The function $\phi : (\mathbb{N}, +) \to (\mathbb{R}, +)$ defined by $\phi(x) = \sqrt{2}x$ is a homomorphism (of binary structures: $(\mathbb{N}, +)$ is not a group!),

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

As before, it is worth spelling this out:

Sum then map $\phi(x + y)$ gives the same result as *map then sum* $\phi(x) + \phi(y)$.

[10] These terms come from ancient Greek: *homo-* (similar, alike), *iso-* (equal, identical), and *morph(e)* (shape, structure).

3. If V, W are vector spaces then every linear map $\mathrm{T} : V \to W$ is a group homomorphism:[11]

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

You've been encountering homomorphisms your entire mathematical career: for instance, both the calculus identity $\frac{\mathrm{d}}{\mathrm{d}x}(f+g) = \frac{\mathrm{d}f}{\mathrm{d}x} + \frac{\mathrm{d}g}{\mathrm{d}x}$ and the distributive law of matrix multiplication $A(\mathbf{x}+\mathbf{y}) = A\mathbf{x} + A\mathbf{y}$ are homomorphism properties!

4. (*Trivial homomorphism*) If G and L are any groups, then the function $\phi : G \to L$ defined by $\phi(g) = e_L$ (the identity in L) is a homomorphism:

$$\forall x, y \in G, \ \ \phi(xy) = e_L = (e_L)^2 = \phi(x)\phi(y)$$

5. (*Inclusion map*) If H is a subgroup of G, then $\phi(x) = x$ defines a homomorphism $\phi : H \to G$:

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

6. The function $\phi(\rho_k) = \rho_{2k \,(\mathrm{mod}\ 4)}$ is a homomorphism $\phi : R_4 \to R_4$:

$$\begin{aligned}\phi(\rho_j \circ \rho_k) &= \phi(\rho_{j+k \,(\mathrm{mod}\ 4)}) = \rho_{2(j+k) \,(\mathrm{mod}\ 4)} = \rho_{2j \,(\mathrm{mod}\ 4)} \circ \rho_{2k \,(\mathrm{mod}\ 4)} \\ &= \phi(\rho_j) \circ \phi(\rho_k)\end{aligned}$$

Establishing Isomorphicity

We must do four things if we suspect binary structures $(G, *)$ and $(H, \star)$ to be isomorphic:

***Definition*:** Define $\mu : G \to H$ and, if necessary, verify that it is a function.[12]
***Homomorphism*:** Verify that $\mu(x * y) = \mu(x) \star \mu(y)$ for all $x, y \in G$.
***Injectivity/1–1*:** Check that $\mu(x) = \mu(y) \implies x = y$.
***Surjectivity/onto*:** Check range $\mu = H$. Equivalently $\forall h \in H$, $\exists g \in G$ such that $h = \mu(g)$.

The last three steps can be done in any order, and injectivity/surjectivity can be combined if you manage to exhibit an explicit *inverse function* $\mu^{-1} : H \to G$. If you are unsure how to start, often the best thing is to play with the homomorphism property itself.

Examples 2.32. 1. We show that $(2\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$ are isomorphic groups.

***Definition*:** The obvious candidate[13] is $\phi(x) = \frac{3}{2}x$. Plainly $\phi(2n) = 3n$ 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 $z = \frac{3}{2} \cdot \frac{2}{3}z = \frac{3}{2}(2n) = \phi(2n) \in \mathrm{range}\,\phi$.

The last steps are essentially the observation that $\phi^{-1}(z) = \frac{2}{3}z$.

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

[11] The scalar multiplication condition $\mathrm{T}(\lambda\mathbf{v}) = \lambda\mathrm{T}(\mathbf{v})$ of a linear map is not relevant here.

[12] If G is a set of equivalence classes, we also need to check that ϕ is *well-defined*. This subtlety is why we haven't (yet) had an example where $\mathbb{Z}_n$ is the *domain* of a homomorphism. We will do so later (Example 3.5.2, Theorem 3.7, etc.).

2. We prove that $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$: these are isomorphic abelian groups (recall that $\mathbb{R}^+ = (0, \infty)$ is the set of *positive real numbers*).

   ***Definition/Homomorphism*:** We need a bijective function $\mu : \mathbb{R} \to \mathbb{R}^+$ which converts addition to multiplication $\mu(x + y) = \mu(x)\mu(y)$. But *exponentiation* does exactly this: defining $\mu(x) = e^x$, we see that the homomorphism property is the familiar exponential law!

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

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

   Other exponential functions also provide suitable isomorphisms: e.g. $2^x, 10^x$, etc.

Demonstrating Non-Isomorphicity (Structural Properties)

Suppose we suspect that binary structures $(G, *)$ and $(H, \star)$ are non-isomorphic. Unless G, H are very small, individually verifying that every possible function $\mu : G \to H$ is a non-isomorphism would be unrealistic! Instead we consider *structural properties*: properties that isomorphic structures must share. If any such is held by one structure but not the other, then the structures are non-isomorphic.

Here is a non-exhaustive list of structural properties; we'll check some in Exercise 11. Throughout, we assume that $\mu : (G, *) \to (H, \star)$ is an isomorphism.

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

***Commutativity & Associativity*:** Suppose $(G, *)$ is commutative and let $X, Y \in H$. Since μ is surjective, we may write $X = \mu(x)$ and $Y = \mu(y)$ for some $x, y \in G$. The homomorphism property now shows that $(H, \star)$ is commutative:

$$X \star Y = \mu(x) \star \mu(y) = \mu(x * y) = \mu(y * x) = \mu(y) \star \mu(x) = Y \star X$$

The argument for associativity is similar, though more tedious.

***Identities & Inverses*:** If $(G, *)$ has identity e, then $\mu(e)$ is the identity for $(H, \star)$. Similarly μ maps inverses to inverses.

***Solutions to equations*:** Related equations have the same number of solutions. For instance,

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

says that the equations $x * x = x$ (in G) and $z \star z = z$ (in H) have the same number of solutions.[14]

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

Examples 2.33. 1. Recall that $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$. Since $(\mathbb{N}_0, +)$ contains the identity element 0 whereas $(\mathbb{N}, +)$ has no identity, we conclude that these binary structures are non-isomorphic.

2. $\mathbb{Z}_5$ is not isomorphic to D_3 since the two groups have different orders (5 and 6).

[13] You might think, "How can I turn an even number into a multiple of three?" Of perhaps you start by thinking about the homomorphism property: multiplication by a constant certainly satisfies $\phi(x + y) = \phi(x) + \phi(y)$.

[14] Such solutions are called *idempotents*; thus existence of idempotents is itself a structural property.

3. The binary structures defined by the two tables are non-isomorphic. For instance, 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

4. $\mathrm{GL}_2(\mathbb{R})$ and $(\mathbb{R}, +)$ are non-isomorphic for the same reason: the first is non-abelian and the second abelian.
5. 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.*
6. The groups $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ have the same (countably infinite) order, and are both abelian. To see that they are non-isomorphic, consider the equation $x + x = 1$ which has no solutions in $\mathbb{Z}$. If $\mu : \mathbb{Z} \to \mathbb{Q}$ were an isomorphism, then the equation $\mu(x) + \mu(x) = \mu(1)$ does have a solution $y = \mu(x) = \frac{1}{2}\mu(1)$ in $\mathbb{Q}$. But then $x = \mu^{-1}(y)$ solves the original equation: contradiction!
7. $(S^1, \cdot)$ and $(\mathbb{R}, +)$ are non-isomorphic: consider the equations $x * x = e$...

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

Suppose $\mu : G \to H$ is a bijection of *sets*, where one of G, H has a binary structure. A binary structure may be *defined* on the other by insisting that μ be an isomorphism.

Example 2.34. The function $\mu(x) = x^3 + 8$ is a bijection $\mathbb{R} \to \mathbb{R}$. Starting with the binary (group) structure $(\mathbb{R}, +)$ and treating μ as an isomorphism, we may create a new isomorphic structure. There are two ways to do this:

***Pull-back*:** Suppose $\mu : (\mathbb{R}, *) \to (\mathbb{R}, +)$. Since $\mu(x * y) = \mu(x) + \mu(y)$, the new operation $*$ must be

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

All structural properties transfer from $(\mathbb{R}, +)$ to $(\mathbb{R}, *)$: for instance, $(\mathbb{R}, *)$ is an abelian group with identity element

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

As a sanity check, observe that we really do have $x * (-2) = \sqrt[3]{x^3 + (-2)^3 + 8} = x$!

***Push-forward*:** View $\mu : (\mathbb{R}, +) \to (\mathbb{R}, *)$ as an isomorphism. Computation of $*$ is an exercise.

"Up to Isomorphism"

This phrase is ubiquitous in group theory. To illustrate, consider that if $(\{e, a\}, *)$ is a group with identity e, then its Cayley table must be as shown (Example 2.10.6). Otherwise said: there may be *infinitely many distinct groups of order two, but all are isomorphic to each other.* This is too wordy, so a mathematician might instead say:

$*$	e	a
e	e	a
a	a	e

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

Make sure you include the snippet "up to isomorphism," for otherwise the sentence is *false*!

The start of group theory can feel very challenging. With its focus on functions and its unfamiliar words, this last introductory section likely seems particularly so. Complete fluency with the vocabulary is *not required* at this stage. The remaining chapters provide plenty opportunity to reinforce the language introduced in this chapter.

For the same reason, several of the following Exercises (particularly number 11 onwards) will likely seem difficult. Try these (and discuss them) now, even if you aren't sure what to do; return later when you feel more comfortable. Learning abstract concepts isn't quick; give the ideas a chance to sink in. By the end of the course, these Exercises *should* seem much easier!

Exercises 2.5. Key concepts: *Homomorphism* *Isomorphism* *Injective/surjective/bijective* *Structural property* *'Up to isomorphism'*

1. Which of the following are homomorphisms/isomorphisms of binary structures? Explain.
   (a) $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +),\ \phi(n) = -n$ (b) $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}, +),\ \phi(n) = n + 1$
   (c) $\phi : (\mathbb{Q}, +) \to (\mathbb{Q}, +),\ \phi(x) = \frac{4}{3}x$ (d) $\phi : (\mathbb{Q}, \cdot) \to (\mathbb{Q}, \cdot),\ \phi(x) = x^2$
   (e) $\phi : (\mathbb{R}, \cdot) \to (\mathbb{R}, \cdot),\ \phi(x) = x^5$ (f) $\phi : (\mathbb{R}, +) \to (\mathbb{R}, \cdot),\ \phi(x) = 2^x$
   (g) $\phi : (\mathrm{M}_2(\mathbb{R}), \cdot) \to (\mathbb{R}, \cdot),\ \phi(A) = \det A$
   (h) $\phi : (\mathrm{M}_n(\mathbb{R}), +) \to (\mathbb{R}, +), \phi(A) = \operatorname{tr} A$ (trace: 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. $\mu(n) = 2 - n$ is a bijection of $\mathbb{Z}$ with itself. For each of the following, define a binary relation $*$ on $\mathbb{Z}$ such that μ is an isomorphism.
   (a) $\mu : (\mathbb{Z}, *) \to (\mathbb{Z}, +)$ (b) $\mu : (\mathbb{Z}, *) \to (\mathbb{Z}, \cdot)$ (c) $\mu : (\mathbb{Z}, *) \to (\mathbb{Z}, \max(a, b))$
5. Finish Example 2.34 by computing the push-forward $X * Y$ for any $X, Y \in \mathbb{R}$.
6. $\mu(x) = x^2$ is a bijection $\mu : \mathbb{R}^+ \to \mathbb{R}^+$. Find $x * y$ if μ is to be an isomorphism.
   (a) $\mu : (\mathbb{R}^+, *) \to (\mathbb{R}^+, +)$ (b) $\mu : (\mathbb{R}^+, +) \to (\mathbb{R}^+, *)$ (c) $\mu : (\mathbb{R}^+, *) \to (\mathbb{R}^+, \cdot)$
7. Show that $x * y = x + y - xy$ is the pull-back of $(\mathbb{R}^\times, \cdot)$ to $\mathbb{R} \setminus \{1\}$ by $\mu(x) = 1 - x$. Use this to provide an alternative quick argument for Exercise 2.1.9.
8. Recall Exercise 2.3.6c. Prove that the Klein four-group and $\mathbb{Z}_8^\times$ are isomorphic.
9. (a) Prove that $S := \left\{ \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{R}) \right\}$ forms a group under matrix addition.
   (b) Prove that $T = S \setminus \{0\}$ (S without the zero matrix) forms a group under matrix *multiplication.*
   (c) Define $\phi \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) = a + ib$. Prove that $\phi : S \to \mathbb{C}$ and $\phi_T : T \to \mathbb{C}^\times$ are *both* isomorphisms
   $$\phi : (S, +) \cong (\mathbb{C}, +), \qquad \phi|_T : (T, \cdot) \cong (\mathbb{C}^\times, \cdot)$$
   (*In a future class, ϕ will be described as an isomorphism of rings/fields*)
10. (Recall Exercise 2.4.8 and Footnote 9) Prove that $S^1 \cong \mathrm{SO}_2(\mathbb{R})$ via an isomorphism
    $$\mu(e^{i\theta}) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

11. Suppose $\mu : (G, *) \to (H, \star)$ is an isomorphism of binary structures. Prove:

    (a) If e is the identity for G, then $\mu(e)$ is the identity for H.

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

    (c) Suppose $\phi : G \to H$ is a *group homomorphism.* Show that parts (a), (b) still hold: $\phi(e_G) = e_H$ and $\phi(x^{-1}) = \big(\phi(x)\big)^{-1}$.
    For a challenge: What happens if ϕ is merely a homomorphism of binary structures?

12. Given a group homomorphism $\phi : G \to H$, define the *image* $\phi(G)$ and *kernel* K as follows:

$$\phi(G) = \operatorname{Im}\phi = \big\{\phi(x) : x \in G\big\}, \qquad K := \big\{x \in G : \phi(x) = e\big\}$$

    (a) Compute the image and kernel of $\phi : (\mathbb{R}^\times, \cdot) \to (\mathbb{R}^\times, \cdot)$ where $\phi(x) = x^2$.

    (b) Prove that $\phi(G)$ is a subgroup of H (in general, not just for the example in (a)!).

    (c) Prove that K is a subgroup of G.

    (*We'll return to these important concepts later*)

13. The groups $(\mathbb{Q}, +)$ and $(\mathbb{Q}^+, \cdot)$ are both abelian and both have the same cardinality: nonetheless, we prove that they are *non-isomorphic.*

    Assume, for contradiction, that $\mu : \mathbb{Q} \to \mathbb{Q}^+$ is an isomorphism.

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

    (b) By considering the number of solutions to the equations in part (a), obtain a contradiction and hence conclude that $(\mathbb{Q}, +) \ncong (\mathbb{Q}^+, \cdot)$.

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

14. Recall the magic square property (Exercise 2.1.11).

    (a) Up to isomorphism, explain why there is a unique group of order three.
    (*This is another reason the groups in Example 2.29 must be isomorphic*!)

    (b) Show that, up to isomorphism, there are precisely two groups of order four.
    (*Hint: 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 group $\mathbb{Z}_4$.*)

    (c) (Hard) What happens for order five?

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

    ***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 & Finite Abelian Groups

In this chapter we consider a general family of groups and see how to combine these to describe any finite abelian group.

3.1 Definitions and Basic Examples

The foundational idea of a cyclic group is that it may be generated from a single element.

Examples 3.1. 1. The integers $(\mathbb{Z}, +)$ are generated by the element 1: all integers may be produced by repeatedly combining 1 using only the group operation $(+)$ and inverses $(-)$. For instance,

$$-4 = -(1+1+1+1)$$

2. The modular arithmetic groups $(\mathbb{Z}_n, +_n)$ (Section 2.3) are also generated by (the remainder) 1. Since the group is finite, inverses are not necessary. For instance,

$$\mathbb{Z}_4 = \{0,1,2,3\} = \{0,\ 1,\ 1+1,\ 1+1+1\}$$

3. The group R_n of rotations of a regular n-gon (Definition 2.24) is generated by the '1-step' rotation ρ_1: that is, $\rho_k = \rho_1^k$.

We formalize this idea by considering the subset of a group that may be produced from a single element, the group operation, and inverses.

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. We call this the cyclic subgroup[15] generated by g.

Proof. We follow the subgroup criterion (Theorem 2.14).

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

***Closure*:** Every element of $\langle g \rangle$ has the form g^k for some $k \in \mathbb{Z}$. The required condition follows from standard exponential notation (Definition 2.3): $g^k \cdot g^l = g^{k+l} \in \langle g \rangle$.

***Inverses*:** This is Exercise 2.1.7c: $(g^k)^{-1} = g^{-k} \in \langle g \rangle$.

■

Definition 3.3 (Cyclic group). A group G is *cyclic* if it has a *generator*: $\exists g \in G$ such that $G = \langle g \rangle$.
In any group G, the *order of an element* g is the order (cardinality) of the cyclic subgroup $\langle g \rangle \leq G$.

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

[15] Since this is an abstract result, the lemma is written multiplicatively. If G is an additive group, then cyclic subgroups are written $\langle g \rangle = \{ng : n \in \mathbb{Z}\} = \{\ldots, -2g, -g, 0, g, 2g, 3g, \ldots\}$. As in Example 3.1.2, for finite cyclic groups convention dictates that the identity element is written first, e.g. $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$.

Examples (3.1 cont). 1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ is generated by either 1 or -1. The cyclic 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. $\mathbb{Z}_n$ is generated by both 1 and $-1 = n - 1$, but may have other generators (we'll consider how to find them all shortly). For instance, $\mathbb{Z}_5$ is generated also by 2:

$$\langle 2 \rangle = \{0, 2,\ 2+2,\ 2+2+2,\ \ldots\} = \{0, 2, 4, 1, 3\} = \mathbb{Z}_5$$

3. $R_n = \langle \rho_1 \rangle = \{e, \rho_1, \rho_1^2, \ldots, \rho_1^{n-1}\}$. As with $\mathbb{Z}_n$, this group typically has other generators.

Another commonly encountered family of cyclic groups arise as subgroups of $(\mathbb{C}^\times, \cdot)$ (or $(S^1, \cdot)$).

Definition 3.4 (Roots of Unity). Let $n \in \mathbb{N}$. The group of n^{th} *roots of unity* U_n is the cyclic subgroup of $(S^1, \cdot)$ generated by $\zeta := e^{\frac{2\pi i}{n}}$:

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

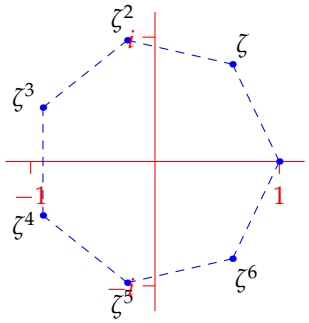
These are precisely the n complex solutions to the equation $z^n = 1$. To emphasize n, write $\zeta_n = e^{\frac{2\pi i}{n}}$.

For instance $U_2 = \langle -1 \rangle = \{1, -1\}$ and $U_4 = \langle i \rangle = \{1, i, -1, -i\}$. In general, the n^{th} roots are the vertices of a regular n-gon centered at 0 with radius 1:

$$\left|\zeta^k\right| = |\zeta|^k = 1 \quad \text{and} \quad \arg \zeta^k = \arg e^{\frac{2\pi k}{n}} = \frac{2\pi k}{n} = k \arg \zeta$$

We stop listing the elements at ζ^{n-1} since $\zeta^n = e^{2\pi i} = 1$. The periodicity of the complex exponential ($e^{i\theta} = 1 \iff \theta \in 2\pi\mathbb{Z}$) results in a simple tie-in with modular arithmetic:

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



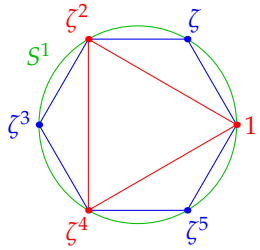
Seventh roots: $\zeta_7 = e^{\frac{2\pi i}{7}}$

Examples 3.5. 1. Observe that $\zeta_6^2 = (e^{\frac{2\pi i}{6}})^2 = e^{\frac{2\pi i}{3}} = \zeta_3$.

This produces a subgroup relationship: writing $\zeta = \zeta_6$, we have

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

The picture makes this geometrically trivial (compare Example 2.26.2).



2. (Example 2.29, cont.) Below is the Cayley table for U_3. Writing $1 = \zeta^0$ and $\zeta = \zeta^1$ makes the isomorphic relationship with $(\mathbb{Z}_3, +_3)$ and $(R_3, \circ)$ obvious: $(U_3, \cdot) \cong (\mathbb{Z}_3, +_3) \cong (R_3, \circ)$.

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

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

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

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

For a little practice here is a formal argument that $\mathbb{Z}_3 \cong U_3$: we show explicitly that

$$\mu : \mathbb{Z}_3 \to U_3 : x \mapsto \zeta^x$$

is an isomorphism. Since the domain $\mathbb{Z}_3$ consists of *equivalence classes*, this requires a little care.

***Well-definition*:** We must prove that if $x = y$ in $\mathbb{Z}_3$, then $\mu(x) = \mu(y)$.
Given $x = y \in \mathbb{Z}_3$, then (*as integers*) $x = y + 3k$ for some integer k. But then

$$\mu(x) = \zeta^x = \zeta^{x+3k} = \zeta^y(\zeta^3)^k = \zeta^y = \mu(y)$$

***Homomorphism*:** $\mu(x+y) = \zeta^{x+y} = \zeta^x\zeta^y = \mu(x)\mu(y)$

***Injectivity*:** $\mu(x) = \mu(y) \implies \zeta^x = \zeta^y \implies \zeta^{x-y} = 1 \implies x \equiv y \pmod 3 \implies x = y$ in $\mathbb{Z}_3$.
(Notice how injectivity is the converse of well-definition!)

***Surjectivity*:** range $\mu = \{\zeta^x : x \in \mathbb{Z}\} = \{1, \zeta, \zeta^2\} = U_3$, since $\zeta^{x+3k} = \zeta^x$.

In the next section we'll essentially repeat this discussion in the abstract, so make sure this example makes sense before moving on.

Exercises 3.1. Key concepts: *Generator* *Order of an element* *Cyclic (sub)group* *Roots of unity*

1. Compute the cyclic subgroup $\langle 12 \rangle$ of $\mathbb{Z}_{20}$ (write the elements in the order generated).
2. Find/describe *all* the generators of each cyclic group.
   (a) $(\mathbb{Z}, +)$ (b) $\{2^n 3^{-n} : n \in \mathbb{Z}\}$ under multiplication
   (c) $(\mathbb{Z}_5, +_5)$ (d) $\left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & b \\ -b & 0 \end{smallmatrix}\right) : a, b = \pm 1 \right\}$ under multiplication
3. State all cyclic subgroups of $\mathbb{Z}_9$. What is the order of each element?
4. Recall Example 2.25. What is the cyclic subgroup of D_3 generated by ρ_1? Generated by μ_1?
5. (a) Find all cyclic subgroups of the Klein four-group V. What is the order of each element?
   (b) V is a *finite* non-cyclic group. Give an example of an *infinite* non-cyclic group, and explain how you know you are correct.
6. Compute the cyclic subgroup $\langle \zeta_8^5 \rangle$ of U_8, listing its elements in the order generated.
7. (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)
8. (a) Show that $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$ forms a cyclic group under *multiplication* modulo 5.
   (b) What about $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ under multiplication modulo 8? To what well-known group is this isomorphic?
9. Suppose that a cyclic group G has order $|G| \geq 3$. Explain why it has *at least two* generators.
10. Modeling Example 3.5.2, prove explicitly that $\mathbb{Z}_n \cong U_n$ for any $n \in \mathbb{N}$.
11. In contrast to the real case (Example 2.32.2), verify that $\phi : \mathbb{C} \to \mathbb{C}^\times : z \mapsto e^z$ is a homomorphism $(\mathbb{C}, +) \cong (\mathbb{C}^\times, \cdot)$ but *not* an isomorphism.

3.2 The Classification and Structure of Cyclic Groups

We describe all cyclic groups, their generators, and subgroup structures.

Lemma 3.6. *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 see that

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

■

The converse is *false*: the Klein four-group V is abelian but not cyclic (Exercise 3.1.5).
The remaining discussion is significantly more abstract: take your time, read carefully, and use the examples to help. We start by observing a pattern you might already have guessed.

Theorem 3.7 (Isomorphs). *Every cyclic group $G = \langle g \rangle$ is isomorphic either to $\mathbb{Z}$ or to some $\mathbb{Z}_n$. Explicitly, $\mu : \mathbb{Z}_{(n)} \to G : x \mapsto g^x$ is an isomorphism: we map generator (1) to generator (g).*

For the purposes of the proof we introduce a set $S := \{m \in \mathbb{N} : g^m = e\}$ of natural numbers ($mg = e$ if G is additive) which helps detect the *order* of G. Here are a few examples of the Theorem.

Examples 3.8. 1. $\mathbb{Z}_4 = \langle 1 \rangle$ is additive, so $S = \{m \in \mathbb{N} : m = 0 \in \mathbb{Z}_4\} = \{4, 8, 12, \ldots\}$. The minimal element 4 is the order of $G = |\mathbb{Z}_4|$.

2. (Example 3.5.2) In $U_3 = \langle \zeta \rangle$, we have $\zeta^m = 1 \iff 3 \mid m$. Plainly $S = \{3, 6, 9, \ldots\}$; its minimal element 3 is the order of U_3. Moreover $\mu(x) = \zeta^x$ is the isomorphism $\mu : \mathbb{Z}_3 \to U_3$ seen before!

3. $5\mathbb{Z} = \langle 5 \rangle$ is an infinite cyclic group. In this case, $S = \{m \in \mathbb{N} : 5m = 0\} = \emptyset$ is *empty*. We have an isomorphism $\mu : \mathbb{Z} \to 5\mathbb{Z} : x \mapsto 5x$ (map the generator 1 of $\mathbb{Z}$ to the generator 5 of $5\mathbb{Z}$).

Proof. We first establish that μ is a bijection. The generic cases depend on the minimal element of S.

Case 1: $S = \emptyset$. Suppose $x > y$ and that $g^x = g^y$. Then $g^{x-y} = e \implies x - y \in S$: contradiction. The elements $\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots$ are *distinct*, and so $\mu : \mathbb{Z} \to G : x \mapsto g^x$ is bijective.

Case 2: $\min S = n$. We first check that $\mu : \mathbb{Z}_n \to G : x \mapsto g^x$ is well-defined:

$$y = x \in \mathbb{Z}_n \implies y = x + kn \text{ for some } k \in \mathbb{Z} \text{ (as integers)}$$
$$\implies \mu(y) = g^y = g^{x+kn} = g^x (g^n)^k = g^x = \mu(x) \qquad (n \in S, \text{ so } g^n = e)$$

This moreover tells us that G is *finite* (there is at most one element of G for each $x \in \mathbb{Z}_n$)

$$G = \langle g \rangle = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\} = \{e, g, \ldots, g^{n-1}\}$$

Now suppose two of these terms were equal; if $0 \leq y \leq x \leq n-1$, then

$$g^x = g^y \implies g^{x-y} = e \implies x = y \qquad (0 \leq x - y \leq n - 1 < n = \min S)$$

We conclude that $G = \{e, g, \ldots, g^{n-1}\}$ has order n, and that μ is a bijection.

To finish the proof, observe that the homomorphism property in both cases is merely standard exponential notation

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

■

The use of S in the proof yields a useful alternative notion of order.

Corollary 3.9 (Order of an element). *If finite, the order of g equals the minimal positive integer n for which $g^n = e$. Moreover $g^m = e \iff n \mid m$.*

Examples 3.10. 1. The group of 7^{th} roots of unity U_7 is isomorphic to $\mathbb{Z}_7$ via $\mu : \mathbb{Z}_7 \to U_7 : k \mapsto \zeta_7^k$. As a sanity check, observe that $7 = \min\{m \in \mathbb{N} : \zeta_7^m = 1\}$ is indeed the order of $\zeta_7 = e^{\frac{2\pi i}{7}}$.

2. $(\mathbb{R}, +)$ is non-cyclic since its (uncountable) cardinality is larger than that of the integers. This is also straightforward directly: if $\mathbb{R} = \langle x \rangle$ were cyclic ($x \neq 0$), then we obtain the contradiction

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

The same argument shows that, for instance, that $(\mathbb{Q}, +)$ is non-cyclic.

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 $\mu : \mathbb{Z} \to G : z \mapsto \xi^z$ is an isomorphism. Multiplication by ξ essentially performs an irrational fraction ($\frac{1}{\sqrt{2}}$) of a full rotation.

Subgroups of Cyclic Groups are also Cyclic!

The motivation for this is simple: for instance, observe that the subgroup $2\mathbb{Z} \leq \mathbb{Z}$ is generated by 2, the *minimal positive integer* in the subgroup. Our goal, given a subgroup $H \leq G = \langle g \rangle$, is to identify a suitable 'minimal' element of H and then demonstrate that this generates H.

Theorem 3.11 (Subgroups of Cyclic Groups). *Any subgroup of a cyclic group is cyclic.*

Proof. Suppose H is a subgroup of $G = \langle g \rangle$. If $H = \{e\}$ is trivial, we are done: $H = \langle e \rangle$ is cyclic! Otherwise, let $s \in \mathbb{N}$ be minimal so that $g^s \in H$ (we may assume $s > 0$ since g^{-s} is also in H). We prove that H is generated by g^s by establishing the set equality $H = \langle g^s \rangle$.

($\supseteq$) This is trivial since $g^s \in H$ and H is a group (closure and inverse axioms of H!).

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

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

Since H satisfies the closure and inverse axioms,

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

The minimality of s forces $r = 0$, from which we conclude that $g^m = (g^s)^q \in \langle g^s \rangle$. ∎

If the proof seems hard, rewrite it for our motivational example: $G = \mathbb{Z}$, $H = 2\mathbb{Z}$ and $s = 2$; remember that G is *additive*, so $(*)$ is simply $r = -2s + m \in 2\mathbb{Z}\ldots$

We finish by considering the finite and infinite cases separately. The later is very simple.

Corollary 3.12 (Subgroups of infinite cyclic groups). *If G is an infinite cyclic group and $H \leq G$, then either $H = \{e\}$ is trivial, or $H \cong G$.*

The proof as an exercise—just generalize the following example!

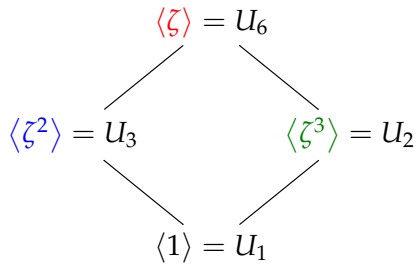
Example 3.13. We write things out explicitly in additive notation when $G = \mathbb{Z}$. By Theorem 3.11, every subgroup has the form $\langle s \rangle = s\mathbb{Z}$ (the multiples of $s \in \mathbb{Z}$). There are two generic situations:

- If $s = 0$ we have the trivial subgroup: $\langle 0 \rangle = \{0\}$.
- If $s \neq 0$, then $s\mathbb{Z}$ is isomorphic to $\mathbb{Z}$ via the isomorphism $\mu : \mathbb{Z} \to s\mathbb{Z} : x \mapsto sx$.

Finite cyclic groups are a little more complicated so we first consider an example.

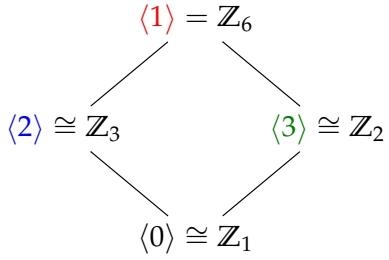
Example 3.14. Consider $U_6 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ under multiplication. Since all subgroups are cyclic, we need only consider the subgroup $\langle x \rangle$ generated by each element x.

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



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	$\{0, 5, 4, 3, 2, 1\}$



Since $U_6 \cong \mathbb{Z}_6$, differences are entirely notational. One subtle distinction is that we don't use *equals* in the second subgroup diagram: for instance, $\langle 2 \rangle = \{0, 2, 4\}$ is *isomorphic* but *not equal* to $\mathbb{Z}_3 = \{0, 1, 2\}$.

As previewed in Lemma 2.21, Example 3.14 should suggest a pattern: the subgroups of $\mathbb{Z}_n$ are precisely those generated by the divisors of n, with one subgroup for each divisor:

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

Our final result merely asserts this for general finite cyclic groups.

Corollary 3.15 (Subgroups of finite cyclic groups). *Let $G = \langle g \rangle$ have order n. For each divisor of n, G has a **unique subgroup** with this order; these are moreover the only subgroups of G.*
More precisely,

$$d = \gcd(s,n) \implies \langle g^s \rangle = \langle g^d \rangle, \quad \text{where this subgroup has order } \tfrac{n}{d} \text{ (isomorphic to } \mathbb{Z}_{\frac{n}{d}})$$

In particular: g^s has order $\frac{n}{\gcd(s,n)}$ and generates G if and only if $\gcd(s,n) = 1$.

Proof. Suppose $d = \gcd(s,n)$. We prove set inclusion in both directions.

($\subseteq$) Since d divides s, we have $s = kd$ for some $k \in \mathbb{Z}$. But then

$$g^s = (g^d)^k \in \langle g^d \rangle \implies (g^s)^t = (g^d)^{kt} \implies \langle g^s \rangle \subseteq \langle g^d \rangle$$

($\supseteq$) Apply Bézout's identity (extended 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, note that since $d \mid n$, there are precisely $\frac{n}{d}$ elements of $\langle g^d \rangle$:

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

■

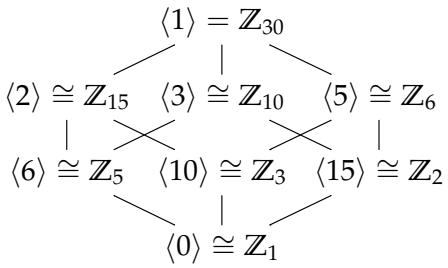
As with Theorem 3.11, rewriting the proof for the special case $G = \mathbb{Z}_n$ might make things clearer. It is more important first to get used to the pattern via *examples*.

Example 3.16. We describe the subgroups of $\mathbb{Z}_{30}$ and construct its subgroup diagram. The first column lists each divisor d of 30 (the possible values of $\gcd(x, 30)$). The second column has the isomorphic group $\mathbb{Z}_{\frac{30}{d}}$, while the third lists the explicit subgroup generated by each $x \in \mathbb{Z}_{30}$.

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

The generators of each subgroup are red in the table. The 'smallest' generator is used for each subgroup in the subgroup diagram.

The *shape* of the subgroup diagram (this one looks something like a cube) depends on the fact that in the *prime decomposition* $30 = 2 \cdot 3 \cdot 5$, each prime appears *exactly once*.



Exercises 3.2. Key concepts: *Every cyclic group isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$*

$\langle g \rangle$ order $n \implies \langle g^s \rangle$ order $\frac{n}{\gcd(s,n)}$ *Subgroup diagrams for finite cyclic groups*

1. Construct the subgroup diagram and give a generator of each subgroup:

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

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

   (a) $n = 5$ (b) $n = 6$ (c) $n = 8$ (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 $\mu : G \to H$ is an isomorphism of cyclic groups. If g is a generator of G, prove that $\mu(g)$ is a generator of H. Do you really need μ to be an *isomorphism* here?
   (b) If G is an infinite cyclic group, how many generators has it got?
   (c) Recall Exercise 3.1.6b. 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.

7. Suppose $G = \langle g \rangle$ is infinite and $H = \langle g^s \rangle$ is an infinite subgroup. Prove Corollary 3.12 by describing an isomorphism $\mu : G \to H$.

8. Prove Corollary 3.9: 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. For which real numbers θ is the multiplicative cyclic group $G = \langle e^{2\pi i\theta} \rangle \leq \mathbb{C}^\times$ finite? Describe the order of G in terms of θ.

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 $X = \{m, n\}$ generates $d\mathbb{Z}$, 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*)

3.3 Direct Products & Finite Abelian Groups

In this section we discuss a straightforward way to create new groups from old using the *Cartesian product*. In the abstract, this discussion applies to any groups, though the ingredients in most of our examples will be cyclic.

Example 3.17. Given $\mathbb{Z}_2 = \{0, 1\}$, the Cartesian product

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

has *four* elements. This set inherits a binary structure via addition of co-ordinates

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

where $x + v$ and $y + w$ are both computed in $(\mathbb{Z}_2, +_2)$. This binary operation has an addition table that should looks very familiar: it has exactly the same structure as 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 type of construction works in general.

Theorem 3.18 (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 group is abelian if and only 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 3.19. 1. The direct product of the groups $(\mathbb{Z}_2, +_2)$ and $(\mathbb{Z}_3, +_3)$ is

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

This is abelian of order 6, so we might guess that it is isomorphic to $(\mathbb{Z}_6, +_6)$ and thus cyclic. This is indeed the case: simply observe that $(1, 1)$ is a generator,

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

In accordance with Theorem 3.7, $\mu(x) = (x, x)$ defines an isomorphism $\mu : \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

2. If each G_k is *abelian* and *written additively*, the direct product is sometimes called a *direct sum*,[16]

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

We won't use this notation, though you've likely encountered it in linear algebra: for instance, 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 3.19.1, we saw that the element $(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ had order 6 and thus generated the group. There is another general pattern here; to help spot it, consider another example.

Example 3.20. We find the order of the element $(10,2) \in \mathbb{Z}_{12} \times \mathbb{Z}_8$? Recall Corollary 3.15:

- $10 \in \mathbb{Z}_{12}$ 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 $(10,2)$ to itself, then the first co-ordinate resets after 6 summations, whereas the second resets after 4. For *both* to reset simultaneously, 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 3.21. *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. We appeal to Corollary 3.9:

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

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

Example 3.22. 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 with reference to Corollary 3.15, the element has order

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

[16] In these notes a direct product/sum will only ever have *finitely many* factors, in which case the concepts are identical. The slight difference in the concepts when there are infinitely many factors is not worth discussing here.

When is a direct product of finite cyclic groups cyclic?

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

Corollary 3.23. *$\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic $\iff \gcd(m,n) = 1$. In such a case $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.*
More generally:

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

Proof. We prove the first part; the generalization follows by induction.

($\Leftarrow$) Suppose $\gcd(m,n) = 1$. We claim that $(1,1)$ is a generator of $\mathbb{Z}_m \times \mathbb{Z}_n$. But this element has order $\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$, so we're done.

($\Rightarrow$) This is Exercise 11. ∎

Examples 3.24. 1. (Example 3.22) The group $\mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_5 \times \mathbb{Z}_{20}$ is non-cyclic since, for instance, $\gcd(4,20) \neq 1$. 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 no pair of 5, 7, 12 have common factors. It is ghastly to write, but there are 12 different ways (up to reordering) of expressing this group as a direct product!

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

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

The Fundamental Theorem of Finite(ly Generated) Abelian Groups

We've used the direct product to create finite abelian groups from cyclic building blocks. While we don't yet have the technology to prove it, our final result provides a powerful converse.

Theorem 3.25. *Every finite abelian group is isomorphic to a group of the form*

$$\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$$

where each $r_j \in \mathbb{N}$ and the p_i are primes (not necessarily distinct). More generally, every finitely generated abelian group (see Exercise 3.2.11) is isomorphic to some

$$\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

Examples 3.26. 1. Up to isomorphism, there are five distinct abelian groups of order $81 = 3^4$:

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

Such groups can often be distinguished by considering the orders of elements. For instance:

$$\left.\begin{array}{ll} G \text{ is abelian of order } 81 & \text{and,} \\ G \text{ has an element of order } 27 & \text{and,} \\ \text{All elements of } G \text{ have order} \leq 27 & \end{array}\right\} \implies G \cong \mathbb{Z}_3 \times \mathbb{Z}_{27}$$

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, maximum order of an element 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 previously, there are multiple isomorphic ways to express each group as a direct product.

We finish by listing, up to isomorphism, all groups of order ≤ 15 and all abelian groups of order 16.

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	$\mathbb{Z}_{16},\ \mathbb{Z}_4 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	(nine)

The Fundamental Theorem & Corollary 3.23 supply the abelian groups. In the non-abelian column:

- The dihedral groups D_n are the familiar symmetries of a regular n-gon (Definition 2.24).
- S_3 and A_4 will be described in Chapter 4 (*symmetric* and *alternating* groups).
- Q_8 is the quaternion group (Exercise 2.2.8). The generalized quaternion group Q_{12} is related.

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. You might suspect from the table that all non-abelian groups have even order: this is not so, though the smallest counter-example has order 21.

Exercises 3.3. Key concepts:

Direct product *Order of an 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 3.18 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 $\mu : \mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$.
   (*Hint: read the proof of Corollary 3.23*)

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. Give a simple explanation for why D_8 is not isomorphic to $\mathbb{Z}_2 \times Q_8$.

11. Complete the proof of Corollary 3.23: 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* $\mathbb{Z}_m \times \mathbb{Z}_n$*?*)

12. 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.

13. (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?

14. 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 prime decomposition of m and the fundamental theorem to identify a suitable subgroup of* $\mathbb{Z}_{p_1^{r_1}} \times \cdot \times \mathbb{Z}_{p_k^{r_k}}$)

15. Suppose G is an abelian group and let $T \subseteq G$ be the subset of elements with *finite order.*

    (a) Prove that T is a subgroup of G.
    (*Your proof shouldn't use the Fundamental Theorem—why not?*)
    (b) Compute T when:
    i. $G = (\mathbb{R}^\times, \cdot)$ ii. $G = (S^1, \cdot)$