Math 120A — Introduction to Group Theory

Neil Donaldson

December 1, 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 $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, 3, \ldots\}$ 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,

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

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

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

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

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 ×.

   (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: $\big(\mathbb{R} \setminus \{1\}, *\big)$ 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 $\big(\mathcal{P}(\mathcal{U}), \triangle\big)$ 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):*

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

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:

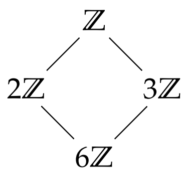
$$1 + 3\mathbb{Z} = \{1 + 3n : n \in \mathbb{Z}\} = \{1, 4, 7, 10, 13, \ldots, -2, -5, -8, \ldots\}$$

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 $(m\mathbb{Z}, +) \le (n\mathbb{Z}, +)$.

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 $K \le H$ and $H \le G$, then $K \le G$.

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):

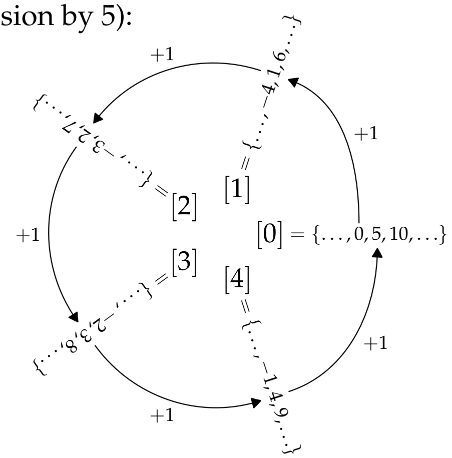
(a) Group/Number Theory style: $4 + 2 = 6 = 1$ in $\mathbb{Z}_5$.

(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 $\mathbb{Z}_4$.

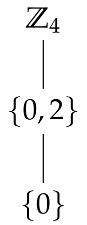
$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\longrightarrow$

$+_4$	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:* $d \mid n \implies \langle d \rangle \leq \mathbb{Z}_n$

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* $\gcd(x, n) = 1 \iff \exists \kappa, \lambda \in \mathbb{Z}$ *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.

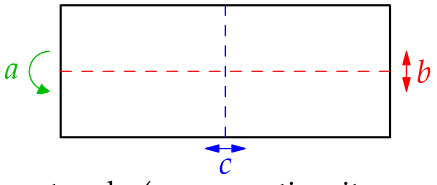
Now consider any geometric figure that has some symmetry (typically viewed as rotational or reflective), such as a triangle, square, or tetrahedron. Each symmetry corresponds to a *function* that transforms the original figure in such a way that the result occupies the same location as the original.

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

(a) Rotation by 180°.

(b) Vertical reflection.

(c) Horizontal reflection.

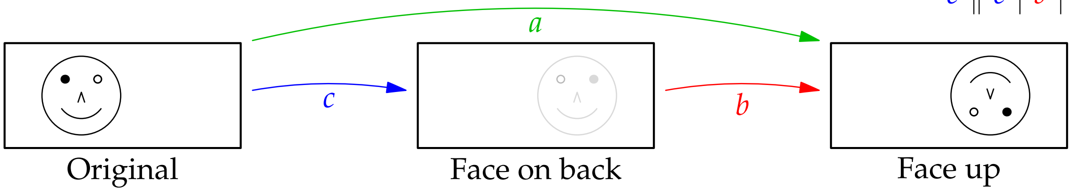


Each symmetry may be viewed as a function transforming the rectangle (or permuting its vertices/edges if you prefer). Group Theorists also consider the *identity function* e as a symmetry: it simply leaves the rectangle alone.[7]

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:

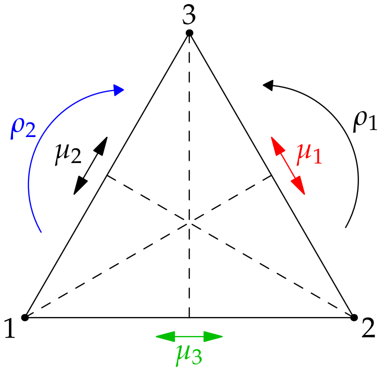
Rotations Labelled $e, \rho_1, \ldots, \rho_{n-1}$ where ρ_k rotates counter-clockwise by $\frac{2\pi k}{n}$ radians ($\frac{360k}{n}{}^\circ$). The identity $e = \rho_0$ is considered a rotation (by 0°).

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!

$\circ$	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 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

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

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

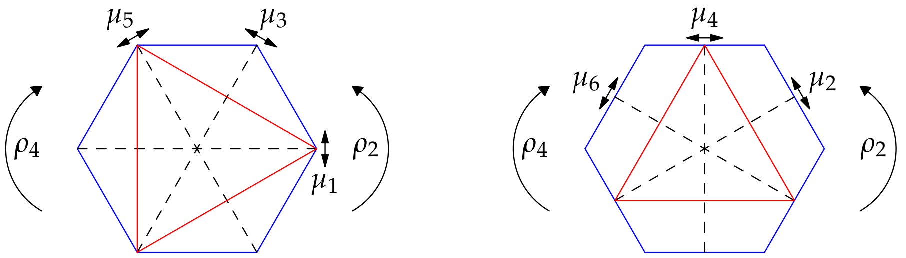
[8] In low dimensions, *orientation-preserving* means that a transformation doesn't change the usual *right-hand rule* (e.g., cross products). In two dimensions these are precisely the *planar rotations*. In three dimensions a general orientation-preserving symmetry is the composition of two pure rotations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

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

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.

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

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

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

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

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

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

$$(AB)^T(AB) = B^TA^TAB = B^TIB = B^TB = I \implies AB \in \mathrm{O}_n(\mathbb{R})$$

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

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

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 $O_2(\mathbb{R})$.

   (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) $\mathcal{K} = \{A \in M_2(\mathbb{R}) : \det A = \pm 1\}$ (b) $\mathcal{L} = \{A \in M_2(\mathbb{R}) : \det A = 7\}$

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

8. Prove that each set of matrices forms a group under multiplication (don't memorize these unless you really love matrices...).

   (a) Special linear group: $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A = 1\}$

   (b) Special orthogonal group: $SO_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : A^T A = I \text{ and } \det A = 1\}$

   (c) $\mathcal{Q}_n = \{A \in M_n(\mathbb{R}) : \det A \in \mathbb{Q}^\times\}$

   (d) (Hard) $SL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : \det A = 1\}$: 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

   $$GL_n(\mathbb{R}), \quad SL_n(\mathbb{R}), \quad O_n(\mathbb{R}), \quad SO_n(\mathbb{R}), \quad \mathcal{Q}_n, \quad SL_n(\mathbb{Z})$$

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 kite-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 $\phi(\rho_k) = \rho_{2k \ (\text{mod } 4)}$ is a homomorphism $\phi : R_4 \to R_4$:

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

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 $z = \frac{3}{2} \cdot \frac{2}{3}z = \frac{3}{2}(2n) = \phi(2n) \in \operatorname{range}\phi$.

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!

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

   ***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.
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.

$*$	a	b
a	a	b
b	b	a

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

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 $x*x=e\ldots$

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 $\big(\{e,a\},*\big)$ 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* $\ker\phi$ as follows:

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

    (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 $\ker\phi$ 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 $(\mathbb{Q}, +) \not\cong (\mathbb{Q}^+, \cdot)$.

    (Extra challenge) Suppose $\phi : (\mathbb{Q}, +) \to (\mathbb{R}, \cdot)$ is a *homomorphism* (of binary structures) 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 $\zeta := e^{\frac{2\pi i}{n}}$:

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

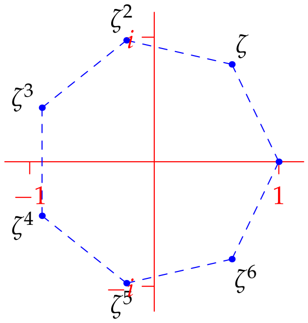
These are precisely the n complex solutions to the equation $z^n = 1$. To emphasize n, write $\zeta_n = e^{\frac{2\pi i}{n}}$.

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:

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



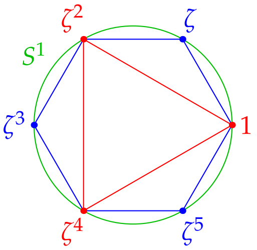
Seventh roots: $\zeta_7 = e^{\frac{2\pi i}{7}}$

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:
   $U_m \le U_n$ 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 $|G| \ge 3$. 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

This section is significantly more abstract that what has come before: take your time, read carefully, and use the examples to help. Our goal is to describe general properties of all cyclic groups, including their generators and subgroup structures. The first result is, mercifully, very simple.

Lemma 3.6. *Every cyclic group is abelian.*

Proof. Let $G = \langle g \rangle$. Any two elements of G can be written g^k, g^l for some $k, l \in \mathbb{Z}$. The result follows from standard exponential notation and the fact that addition of integers is commutative:

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

■

Note that the converse is *false*: the Klein four-group V is abelian but not cyclic (Exercise 3.1.5).

Our major classification theorem proves a pattern you've likely already guessed.

Theorem 3.7 (Isomorphs). *Every cyclic group $G = \langle g \rangle$ is isomorphic either to $\mathbb{Z}$ or to some $\mathbb{Z}_n$:*

- *If G is infinite, then $G \cong \mathbb{Z}$.*
- *If G is finite with order n, then $G \cong \mathbb{Z}_n$.*

In either case, $\mu : \mathbb{Z}_{(n)} \to G : x \mapsto g^x$ is an explicit isomorphism.

To help understand the theorem and set up the proof, some remarks and examples are helpful.

Map Generator to Generator The isomorphism maps the generator $1 \in \mathbb{Z}_{(n)}$ to the generator g of G. Together with the homomorphism property, this idea *defines* μ

$$\mu(1) = g \implies \mu(x) = \mu(x + \cdots + x) = \big(\mu(1)\big)^x = g^x$$

This observation makes it easy to find suitable isomorphisms in examples.

***The* Cyclic Group of Order n?** The theorem says that, *up to isomorphism*, there is a unique cyclic group of order n. For this reason, many algebraists use the symbol $\mathbb{Z}_n$ (or C_n for 'cyclic') to refer to any example of a cyclic group of order n (e.g. R_n, U_n, etc.). For clarity, in these notes, $\mathbb{Z}_n$ will always be the explicit group of remainders under addition modulo n.

The Order of $G = \langle g \rangle$ It is helpful to introduce a set of positive integers

$$S := \{m \in \mathbb{N} : g^m = e\} \qquad (mg = e \text{ if } G \text{ is additive})$$

This set plays a crucial role in the proof, distinguishing the finite/infinite cases and detecting the order of G...

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 plainly the order of $|\mathbb{Z}_4|$.

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

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:

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

This moreover tells us that G is *finite* (there are at most n distinct elements of G)

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

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

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

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

Finally, note that the homomorphism property in both cases is merely standard exponential notation

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

■

As advertised, the use of S in the proof yields a useful alternative notion for the order of an element.

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 $g^m = e \iff n \mid m$.*

Otherwise said, if g has order n, then $S = \{m \in \mathbb{N} : g^m = e\} = \{kn : k \in \mathbb{N}\}$ is the set of positive multiples of n.

Examples 3.10. 1. The group of 7th 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

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

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!

For the remainder of this section we describe the complete subgroup structure of all cyclic groups. Our approach is motivated by a simple example.

Example 3.11. The cyclic subgroup $2\mathbb{Z} \leq \mathbb{Z}$ is generated by 2: the *minimal positive integer* in the subgroup.

For an abstract subgroup H of a cyclic group $G = \langle g \rangle$, our goal is to identify a suitable 'minimal element' of H and then demonstrate that this generates H.

Theorem 3.12 (Subgroups of Cyclic Groups). *Every subgroup of a cyclic group is cyclic.*

Proof. Suppose H is a subgroup of $G = \langle g \rangle$. Let s be the smallest *positive* integer[16] such that $g^s \in H$. We prove that H is generated by g^s by establishing the set equality $H = \langle g^s \rangle$.

($\supseteq$) Since H is a group, the closure and inverse axioms force $(g^s)^k \in H$ for all $k \in \mathbb{Z}$.

($\subseteq$) Let $g^m \in H$. We must prove that $g^m \in \langle g^s \rangle$. 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,

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

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, try rewriting it for our motivational example, where $G = \mathbb{Z}$, $H = 2\mathbb{Z}$ and $s = 2$; remember that G is *additive*, so $(*)$ is simply $r = -2s + m \in 2\mathbb{Z}$!

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

Corollary 3.13 (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 generic example!

Example 3.14. We write things out explicitly in additive notation when $G = \mathbb{Z}$. By Theorem 3.12, 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 $\mu : \mathbb{Z} \to s\mathbb{Z} : x \mapsto sx$.

[16] This exists for two reasons:

1. H is a non-empty subset of $G = \langle g \rangle$ and so must contain some element g^k. We may assume $k \geq 1$ since the subgroup also contains g^{-k} (inverse axiom).
2. The set of natural numbers $\{k \in \mathbb{N} : g^k \in H\}$ is non-empty and so (well-ordering) has a minimal element s.

Note that $s = 1 \iff H = \langle e \rangle$ is the trivial subgroup ($g^1 = e^1 = e \in H$). In this special case the division algorithm argument is trivial: every $m = q \cdot 1 + 0$ is immediately a multiple of 1, and $g^m = e$ for all m.

Finite cyclic groups are more complicated, so we first illustrate the main result with an example.

Example 3.15. Consider the 6th roots of unity $U_6 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$. Since every subgroup of U_6 is necessarily cyclic (Theorem 3.12), it is enough to consider each cyclic subgroup $\langle z \rangle$ in turn (for each $z \in U_6$). We obtain three proper subgroups, as arranged in the subgroup diagram below.

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

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

Observe the repetitions: $\langle \zeta \rangle = \langle \zeta^5 \rangle = U_6$ and $\langle \zeta^2 \rangle = \langle \zeta^4 \rangle = U_3$. Note also that we really do have *equality* of groups here: for instance, $\zeta^2 = (e^{\frac{2\pi i}{6}})^2 = e^{\frac{2\pi i}{3}}$ is a generator of U_3.

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

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

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

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 $\mathbb{Z}_3 = \{0, 1, 2\}$.

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

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

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

Corollary 3.16 (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,

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

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

As with Theorem 3.12, if the proof seems hard, try rewriting it when $G = \mathbb{Z}_n$.

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 $\langle g^d \rangle$:

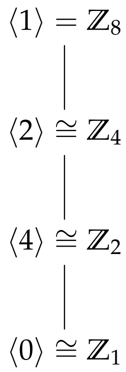
$$\langle g^d \rangle = \{e, g^d, g^{2d}, \ldots, g^{n-d}\}$$

■

Example 3.17. 1. $\mathbb{Z}_8$ is generated by $1, 3, 5$ and 7: precisely the elements for which $\gcd(s, 8) = 1$. For example,

$$\langle 5 \rangle = \{5, 2, 7, 4, 1, 6, 3, 0\} = \mathbb{Z}_8$$

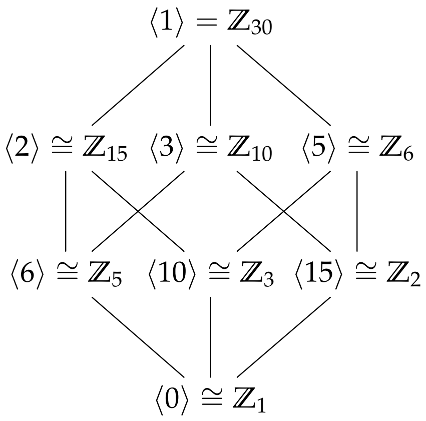
Similarly, the subgroup $\langle 6 \rangle = \{6, 4, 2, 0\}$ has order $4 = \frac{8}{\gcd(6,8)}$. The complete collection of subgroups is in the table: the first column lists each divisor d of 8 (the possible values of $\gcd(x, 8)$), while the second column has the explicit subgroup generated by each x, and the group isomorph $\mathbb{Z}_{\frac{8}{d}}$. The 'smallest' generator is used for each subgroup in the subgroup diagram.


$\langle 1 \rangle = \mathbb{Z}_8$
$\langle 2 \rangle \cong \mathbb{Z}_4$
$\langle 4 \rangle \cong \mathbb{Z}_2$
$\langle 0 \rangle \cong \mathbb{Z}_1$

$d = \gcd(x, 8)$	Subgroup $\langle x \rangle \cong \mathbb{Z}_{\frac{8}{d}}$
1	$\{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8$
2	$\{0, 2, 4, 6\} \cong \mathbb{Z}_4$
4	$\{0, 4\} \cong \mathbb{Z}_2$
8	$\{0\} \cong \mathbb{Z}_1$

2. We repeat the discussion for $\mathbb{Z}_{30}$.

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


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

You should consider how the *shape* of the subgroup diagram for $\mathbb{Z}_n$ depends on the *prime decomposition* of n: for instance, each prime appears exactly once in $30 = 2 \cdot 3 \cdot 5$.

Exercises 3.2. Key concepts: *Every cyclic group is isomorphic to* $\mathbb{Z}$ *or* $\mathbb{Z}_n$ $\quad g^m = e \iff (\operatorname{ord} g) \mid m$

$\langle g\rangle \cong \mathbb{Z}_n \implies \langle g^s\rangle \cong \mathbb{Z}_{\frac{n}{\gcd(s,n)}}$ *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 4th 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 3.13 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 3.18. 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 3.19 (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 3.20. 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*,[17]

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

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 3.20.1, 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 3.21. We find the order of the element $(10,2) \in \mathbb{Z}_{12} \times \mathbb{Z}_8$? Recall Corollary 3.16:

- $10 \in \mathbb{Z}_{12}$ 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* $12 = \text{lcm}(6,4)$.

Theorem 3.22. *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 $\text{lcm}(r_1,\ldots,r_n)$.*

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 $m = \text{lcm}(r_1,\ldots,r_n)$. ■

Example 3.23. 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 3.16, the element has order

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

[17] 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 3.24. *$\mathbb{Z}_m \times \mathbb{Z}_n$ 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 3.25. 1. (Example 3.23) 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

Direct products create finite abelian groups from cyclic building blocks. Our final result provides a powerful converse, though we don't have the technology to prove it (yet—though see Section 7.3).

Theorem 3.26. *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 3.27. 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:

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

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 3.24 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 of finitely generated abelian groups

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 3.19 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 3.24*)

8. State three non-isomorphic groups of order 50.

9. Let p, q be distinct primes. Up to isomorphism, how many abelian groups have 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 3.24: 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 finite abelian and that m divides $|G|$. Prove that G has a subgroup of order m.
    (*Hint: use the prime decomposition of m and the Fundamental Theorem*)

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. $G = (S^1, \cdot)$

4 Permutations and Orbits

In this chapter we return to the origins of group theory by considering the ways in which a set may be reordered.

4.1 The Symmetric Group, Cycle Notation & Cayley's Theorem

Definition 4.1. Let A be a set. A *permutation* of A is a bijective/invertible function $\sigma : A \to A$.
The *symmetric group* S_A is the set of all permutations of A under functional composition.
The *symmetric group on n-letters*[18] S_n is the group S_A when $A = \{1, 2, \ldots, n\}$.

Examples 4.2. 1. If $A = \{1\}$, there is only one (bijective) function $A \to A$, namely the *identity function* $e : 1 \mapsto 1$. Thus S_1 has only one element and is isomorphic to $\mathbb{Z}_1$.

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

$\circ$	e	σ
e	e	σ
σ	σ	e

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

3. $S_3 = S_{\{1,2,3\}}$ has *six elements* and is *non-abelian*. We have met this group before: note how every rotation/reflection of the triangle in Example 2.25 corresponds to a permutation of the three vertices 1, 2, 3. Otherwise said, S_3 is isomorphic to the dihedral group D_3.

Lemma 4.3. 1. *S_A is a group under composition of functions.*

2. *If A has at least three elements, then S_A is non-abelian.*

3. *The order of S_n is $n!$* *(Warning! The order of S_n is not the subscript n)*

4. *$S_m \leq S_n$ whenever $m \leq n$* *(Strictly, S_n contains a subgroup* isomorphic *to S_m)*

Proof. 1. The axioms follow from familiar function properties. Write out the details if you're unsure.

Closure: If $\sigma, \tau : A \to A$ are bijective, so is the composition $\sigma \circ \tau$.

Associativity: Composition of functions is associative (Exercise 2.4.9).

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

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

The remaining parts are exercises. ∎

From now on we use juxtaposition: $\sigma\tau := \sigma \circ \tau$. Exponentiation therefore means self-composition: e.g. $\sigma^3 = \sigma\sigma\sigma = \sigma \circ \sigma \circ \sigma$. Remember also that $\sigma\tau$ is a *function* $A \to A$, and that evaluation means that we act with τ first:

$$\forall a \in A, \ \sigma\tau(a) = \sigma\big(\tau(a)\big)$$

[18] This choice of A makes S_n explicit. In practice, any set with n elements will do and any group isomorphic to this is usually also called S_n (see Exercise 8 and the remark regarding "up to isomorphism" on Page 20).

Cycle Notation

Efficient computation in S_n is facilitated by some new notation.

Definition 4.4. Suppose $\{a_1, \ldots, a_k\} \subseteq \{1, \ldots, n\}$. The *$k$-cycle* $\sigma = (a_1\, a_2 \cdots a_k) \in S_n$ is the function

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

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

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

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

Example 4.5. A 4-cycle $\sigma = (1\,3\,4\,2)$ and a 2-cycle $\tau = (1\,4)$ in S_4 are defined in the table:

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

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

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

To compose cycles, remember that both are *functions* and you won't go wrong!

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

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

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

Algorithmic Cycle Composition Computation using tables is impractically slow. Here is an algorithmic approach that, with practice, should prove more efficient. We illustrate by verifying the previous calculation: at each stage we write only a single number or bracket, building up the right column below.

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

It should be clear how to extend the algorithm when composing more cycles. Any 1-cycles obtain should be deleted. Shortly we'll prove that the algorithm always terminates in a product of disjoint cycles (Theorem 4.13). For now, practice it by verifying the following:

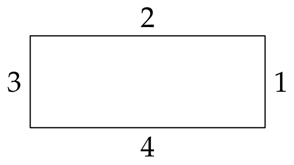
Examples 4.6. 1. $(1\,4)(1\,3\,4\,2) = (1\,3)(2\,4)$ 2. $(1\,3\,5\,4)(2\,3\,4) = (1\,3)(2\,5\,4)$

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

Geometric Symmetry Groups (Section 2.4 revisited)

We've already seen (Example 4.2.3) how the symmetry group D_3 of an equilateral triangle is isomorphic to the symmetric group S_3. The same trick applies more generally: label the vertices (or edges/faces) of a figure with numbers $1, 2, 3, \ldots$ and represent each rotation/reflection by how it permutes these values. Cycle notation makes calculating compositions easy!

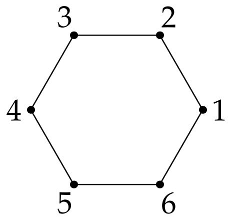
Examples 4.7. 1. Label the edges of a rectangle to view the Klein four-group V as a subgroup of S_4: the 2-cycles $(1\,3)$ and $(2\,4)$ are reflections, and their composition is rotation by 180°.



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

Alternative descriptions of V can be obtained by using different labellings (Exercise 3).

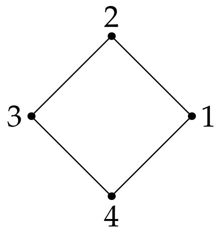
2. Label the vertices of a regular hexagon 1 through 6.



- The 2,2-cycle $(1\,5)(2\,4)$ represents reflection across the line through 3 and 6.
- The 6-cycle $(1\,2\,3\,4\,5\,6)$ represents 60° counter-clockwise rotation.

Both functions describe elements of the dihedral group D_6. By extension, D_6 may be identified as (is isomorphic to) a subgroup of S_6.

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

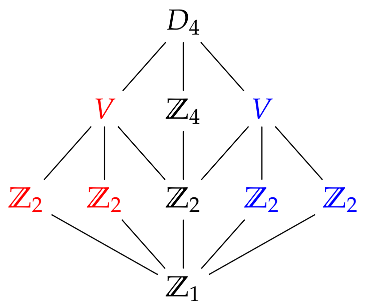


Note the ease of computations: e.g.,

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

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

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



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

The same thing can be done for 3D figures like the tetrahedron (Example 4.26.3).

Cayley's Theorem

The word *group*, at least in mathematics, originally referred to a set of permutations. We finish this section with a foundational result that links to the original meaning of the word: every element of a group may be viewed as a permutation—indeed of the group itself!

Theorem 4.8 (Cayley). *Every group is isomorphic to a group of permutations.*

The proof of Cayley's Theorem is merely the abstraction of a simple example.

Example 4.9. To each integer g, we may associate the *function* "add g." For instance, 1 corresponds to the function "+1," etc. The function "add g" is a bijection of the integers: its inverse function is "add $-g$." Each integer is therefore naturally associated to a *permutation*, an element of the group $S_{\mathbb{Z}}$.

Proof. Let G be a group. For each $g \in G$, define *left-multiplication by g* to be the function $L_g : G \to G$ where,

$$\forall x \in G,\ L_g(x) = gx$$

This is bijective (inverse function $(L_g)^{-1} = L_{g^{-1}}$), and therefore a *permutation* of G: that is $L_g \in S_G$. Now define a function $\phi : G \to S_G$ by $\phi(g) = L_g$. We prove that ϕ is an injective homomorphism.

Injectivity $\phi(g) = \phi(h) \implies L_g = L_h \implies L_g(e) = L_h(e) \implies ge = he \implies g = h$

Homomorphism We show that $\phi(gh) = \phi(g)\phi(h)$ *as functions* by evaluating on all $x \in G$:

$$\big(\phi(gh)\big)(x) = L_{gh}(x) = (gh)x = g(hx) = L_g\big(L_h(x)\big) = \big(\phi(g)\phi(h)\big)(x)$$

By Exercise 2.5.12, ϕ is an *isomorphism* onto its image/range. Otherwise said, G is isomorphic to the subgroup $\phi(G)$ of the symmetric group S_G. ∎

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

Exercises 4.1. Key concepts: *Permutation* *Symmetric group* *Cycle notation*

1. Which of the following functions are permutations? Explain.

   (a) $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x) = x - 7$.
   (b) $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x) = -3x + 4$.
   (c) $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^3 - x$.
   (d) $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^3 + x$.
   (e) $f : \{\text{fish, horse, dog, cat}\} \to \{\text{fish, horse, dog, cat}\}$ where

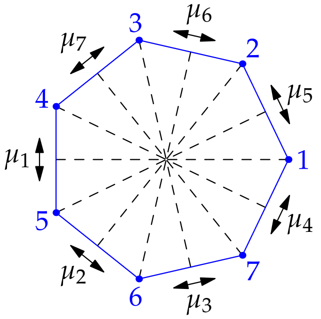
   $$f(\text{fish}) = \text{horse}, \quad f(\text{horse}) = \text{cat}, \quad f(\text{dog}) = \text{dog}, \quad f(\text{cat}) = \text{fish}$$

2. Compute the following products (compositions) of permutations in cycle notation.

   (a) $(1\,2)(3\,4)(1\,2\,3) \in S_4$
   (b) $(1\,4)(2\,3)(3\,4)(1\,4) \in S_4$
   (c) $(1\,2\,3)(2\,3\,4)(3\,4\,1)(4\,1\,2) \in S_4$
   (d) $(1\,2\,4\,5)^2(2\,4\,5)^2 \in S_5$

3. (Example 4.7.1, cont.) Use different labellings of the edges of the rectangle to find another two subgroups of S_4 isomorphic to V. What happens if you instead label the rectangle's *vertices*?

4. By labelling vertices, view the dihedral group D_7 of symmetries of the regular heptagon as a subgroup of S_7. Each μ_i is reflection across the indicated dashed line, while ρ_j is rotation j steps counter-clockwise.



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

   (a) State μ_4 in cycle notation.

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

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

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

6. Prove parts 2, 3, and 4 of Lemma 4.3.

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

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

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

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

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

10. In Cayley's Theorem we defined $\phi(g) = L_g : G \to G$ via *left-multiplication.*

   (a) Does the argument still work if $\phi(g) = R_g : G \to G$ is *right-multiplication* $R_g(x) = xg$?

   (b) (Harder) Suppose we take $\phi(g) = C_g : G \to G$ to be the function $C_g(z) = gxg^{-1}$. Does the proof of Cayley's Theorem work this time? Why/why not?

11. Show that the group S_3 is *indecomposable*: there are no groups G, H of order less than $|S_3| = 6$ for which $S_3 \cong G \times H$.

    (*Hint: If S_3 is decomposable, there is only one possibility; why does this decomposition make no sense?*)

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

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

13. (a) Let $\mu \in D_n$ be a reflection and ρ the one-step counter-clockwise rotation. Prove that $\mu\rho = \rho^{n-1}\mu$ and more generally that $\mu\rho^k = \rho^{n-k}\mu$.

   (b) Define a group G abstractly as the elements generated by objects ρ, μ with the properties:

$$\rho \text{ has order } n, \quad \mu \notin \langle\rho\rangle \text{ has order 2}, \quad \text{and } \mu\rho = \rho^{n-1}\mu$$

   Prove that $G = \{e, \ldots, \rho^{n-1}, \mu, \ldots, \rho^{n-1}\mu\}$ has order $2n$, and that each $\rho^k\mu$ has order 2.

   (In many textbooks this is the *definition* of D_n.)

4.2 Orbits

Group theory is often applied by allowing the elements of a group to transform a set.[19] We've already seen several examples: for instance, how rotations transform a geometric figure. The simplest general example is built into the definition of the symmetric group and appears naturally in cycle notation.

Definition 4.10. The *orbit* of $\sigma \in S_n$ containing $x \in \{1, 2, \ldots, n\}$ is the *set*

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

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

Examples 4.11. If $\sigma \in S_n$ is written as a product of *disjoint cycles*, then the cycles are the orbits.

1. The orbits of $(1\,3\,4) \in S_4$ are the disjoint sets $\{1, 3, 4\}, \{2\}$. Note the singleton orbit $\{2\}$!
2. The orbits of $(1\,2)(4\,5) \in S_5$ are $\{1, 2\}, \{3\}, \{4, 5\}$.
3. Non-disjoint cycles are not orbits. For instance, $\sigma = (1\,3)(2\,3\,4) \in S_4$ maps

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

   so there is only one orbit: $\text{orb}_x(\sigma) = \{1, 2, 3, 4\}$ for any x. This comports with the result obtained by multiplying cycles via the usual algorithm: $\sigma = (1\,2\,3\,4)$.

Given that disjoint cycle notation is so useful for reading orbits, it is natural to ask if *any* permutation can be written in such a manner. The answer is yes, as we demonstrate in the next two results.

Lemma 4.12. *The orbits of $\sigma \in S_n$ partition $X = \{1, 2, \ldots, n\}$.*

Proof. Define a relation $\sim$ on $X = \{1, 2, \ldots, n\}$ by $x \sim y \iff y \in \text{orb}_x(\sigma)$. We claim that this is an equivalence relation.[20]

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

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

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

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

[19] The formal definition of such *group actions* is postponed until Chapter 7.

[20] The relationship between equivalence relations and partitions underpins several upcoming ideas, and *should* be familiar from a previous course. Here is a very quick review:

Given $x \in X$ and a relation $\sim$ on X, define the set $[x] := \{y \in X : y \sim x\}$.

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

In our situation, $[x] = \text{orb}_x(\sigma)$; the Lemma simply proves that the orbits of σ are equivalence classes.

Theorem 4.13. *Every permutation can be written as a product of disjoint cycles.*

Proof. We formalize the algorithm from page 38. Suppose $\sigma \in S_n$ is given.

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

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

   If this all of $X = \{1, \ldots, n\}$, we are finished: $\sigma = \big(1\ \sigma(1)\ \sigma^2(1)\ \ldots\ \sigma^{n-1}(1)\big)$ is an n-cycle.

2. Otherwise, let $x_2 = \min\{x \in X : x \notin \text{orb}_1(\sigma)\}$ and construct its orbit:

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

   By Lemma 4.12, $\text{orb}_{x_2}(\sigma)$ is disjoint with $\text{orb}_1(\sigma)$. If $\text{orb}_1(\sigma) \cup \text{orb}_{x_2}(\sigma) = X$ then we are done, and σ is the product of two disjoint cycles:

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

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

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

The Theorem explains why our cycle algorithm always produces a product of disjoint cycles! By convention, $1 < x_2 < \cdots < x_k$, though there is no need to do this: disjoint cycles can be listed in any order and may start with any element, e.g.,

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

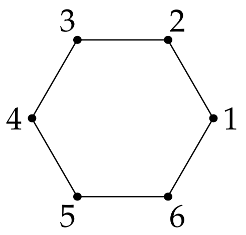
Also, by convention, we delete any orbits of size 1 (1-cycles).

Orders of Elements in S_n

Recall (Corollary 3.9) that the order of an element $\sigma \in S_n$ is the smallest positive integer k for which $\sigma^k = e$.

Example 4.14. If $\sigma = (1\,2\,3\,4\,5\,6) \in S_6$, then

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



whence the order of σ is 6. This is intuitive if we identify σ with a counterclockwise rotation of a regular hexagon: indeed $\langle\sigma\rangle = \{e, \sigma, \ldots, \sigma^5\} \cong R_6$.

By similarly considering a regular k-gon, it should be clear that every k-cycle has order k.

Things are trickier when you don't have a single cycle. However, we are again saved by the discussion of disjoint cycles, since *disjoint cycles commute.*

Examples 4.15. 1. Since $(1\,2\,3)$ and $(4\,5)$ are disjoint cycles, we know that $(1\,2\,3)(4\,5) = (4\,5)(1\,2\,3)$. We therefore easily compute

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

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

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

but this would be incorrect: the *cycles don't commute* $(2\,5\,3)(1\,5\,4\,3) \neq (1\,5\,4\,3)(2\,5\,3)$ so we cannot distribute the exponent (8). If instead we first find σ as a product of disjoint cycles, then the exponent does distribute and the computation is easy

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

This approach also tells us the order of σ. Observe that

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

The order if σ is therefore 6.

Corollary 4.16. *The order of a permutation σ is the least common multiple of the lengths of its disjoint cycles.*

Proof. Write $\sigma = \sigma_1 \cdots \sigma_m$ as a product of disjoint cycles, where the cycle σ_j has length α_j. Since disjoint cycles commute,

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

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

$$\sigma^k = e \iff \forall j,\ \sigma_j^k = e \iff \forall j,\ \alpha_j \mid k \qquad \text{(the order of an } \alpha_j\text{-cycle is } \alpha_j)$$

The order of σ is the smallest k satisfying this condition, namely $\operatorname{lcm}(\alpha_1, \ldots, \alpha_m)$. ■

Example 4.17. Since $\sigma = (1\,4\,5)(3\,6\,2\,7)(8\,9) \in S_9$ is written as a product of disjoint cycles, its order is $\operatorname{lcm}(3, 4, 2) = 12$.

To compute σ^{3465}, first observe that $3465 = 12 \cdot 288 + 9$ (division algorithm). From this,

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

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

Exercises 4.2. Key concepts: *Orbit* *Partition* *Disjoint cycles* *Order of element via lcm*

1. Find the orbits of the following permutations, and their orders:

   (a) $\rho = (1\,4\,5)(2\,3\,4\,5) \in S_5$.

   (b) $\sigma = (1\,5\,4)(2\,5\,4)(1\,2\,3\,4) \in S_5$.

   (c) $\tau = (1\,5\,7\,4)(3\,2\,4)(3\,2\,5\,6) \in S_7$.

2. If $\sigma \in S_A$ is any permutation, we may define its orbits similarly: $\text{orb}_a(\sigma) = \{\sigma^j(a) : j \in \mathbb{Z}\}$. What are the orbits of the permutation $\sigma : \mathbb{Z} \to \mathbb{Z} : n \mapsto n+3$?

3. Given $\sigma = (1\,3)(2\,4\,5) \in S_5$, find the elements of the cyclic group $\langle\sigma\rangle \leq S_5$ generated by σ.

4. What is the largest possible order of an element of the group $S_3 \times \mathbb{Z}_4 \times V$? Exhibit one.

5. What is the maximum order of an element in each of the groups S_4, S_5, S_6, S_7, S_8? Exhibit a maximum order element in each case.

6. For which integers n does there exist a subgroup $C_n \leq S_8$ where C_n is cyclic of order n? Explain your answer.

7. Let $\sigma \in S_n$. For each $k > 0$, prove that each orbit of σ^k is a subset of an orbit of σ.

8. Consider the permutations $\sigma = (1\,3\,5)(2\,7\,4\,9\,6)$ and $\tau = (1\,5\,3\,2)(6\,9)$ in S_9.

   (a) Compute $\sigma\tau$ and $\tau\sigma$ in cycle notation.

   (b) Find the orders of σ, τ, $\sigma\tau$ and $\tau\sigma$.

   (c) Compute $(\sigma\tau)^{432}\sigma^{43}$ as a product of disjoint cycles.

   (d) Construct the subgroup diagram of $\langle\sigma\rangle$ and give a generator for each subgroup.

4.3 Transpositions & the Alternating Group

In the previous sections we viewed a permutation in terms of its orbits. An alternative approach involves the construction of permutation from the very simplest bijections.

Definition 4.18. A 2-cycle $(a_1\,a_2)$ is also known as a *transposition*, since it swaps two elements of $\{1,2,\ldots,n\}$ and leaves the rest untouched.

Theorem 4.19. *Every $\sigma \in S_n$ $(n \geq 2)$ may be written as a product of transpositions.*

Proof. There are many, many ways to do this. One approach is first to write σ as a product of disjoint cycles, before decomposing each cycle as follows:

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

Just read carefully and you should be convinced this works! ■

Example 4.20. The method in the proof results in the decomposition

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

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

While representations as a product of transpositions are non-unique, a simple commonality may be observed via *matrix notation*. Consider, for instance,

$$\begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix}\begin{pmatrix}a\\b\\c\\d\end{pmatrix}=\begin{pmatrix}a\\d\\c\\b\end{pmatrix} \quad\text{and}\quad \begin{pmatrix}0&0&1&0\\0&0&0&1\\0&1&0&0\\1&0&0&0\end{pmatrix}\begin{pmatrix}a\\b\\c\\d\end{pmatrix}=\begin{pmatrix}c\\d\\b\\a\end{pmatrix}$$

Each of these 4×4 matrices *permutes* the rows of any $4 \times k$ matrix following it. These matrices correspond naturally to two elements of S_4:

- The transposition $(2\,4)$ (swap rows 2 and 4).
- The 4-cycle $(1\,4\,2\,3)$ (map row 1 to row 4, row 4 to row 2, etc.)

Definition 4.21. A *permutation matrix* is square matrix which is zero except for a single 1 in each row and column. Equivalently, it is obtained by permuting the *rows* of the identity matrix.

Lemma 4.22. *The set of $n \times n$ permutation matrices forms a multiplicative group isomorphic to S_n.*

We omit a formal proof, though the rough idea is hopefully clear: replace each $\sigma \in S_n$ with its corresponding permutation matrix and observe that composition corresponds to matrix multiplication.

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

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

and view this as a product of matrices, taking determinant of both sides shows that

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

The value of the determinant plainly depends only on whether m is *even* or *odd*…

Definition 4.23. A permutation $\sigma \in S_n$ is *even/odd* if it can be written as the product of an even/odd number of transpositions.

By our matrix/determinant discussion, the parity of a permutation is well-defined: every permutation is either even or odd; it cannot be both!

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

Definition 4.24. The *alternating group* A_n $(n \geq 2)$ is the group of even permutations in S_n.

Theorem 4.25. *A_n contains exactly half the elements of S_n: otherwise said, $|A_n| = \frac{n!}{2}$.*

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

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

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

Examples 4.26. We describe the smallest three alternating groups A_4.

1. $A_2 = \{e\} \cong \mathbb{Z}_1$ is trivial.

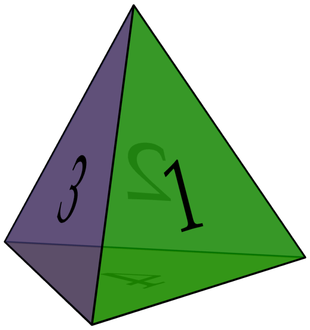
2. $A_3 = \{e, (1\,3)(1\,2), (1\,2)(1\,3)\} = \{e, (1\,2\,3), (1\,3\,2)\} \cong \mathbb{Z}_3$ is a cyclic group.

3. When $n = 4$ we obtain the first 'new' group in the alternating family; a group of order 12.

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

A_4 is non-abelian: for example,

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



While we've already countered one non-abelian group of order 12, the dihedral group D_6, we quickly see that $A_4 \ncong D_6$: all elements of A_4 have orders 1, 2 or 3, while D_6 contains a rotation (by 60°) of order 6.

By labelling faces (or vertices), A_4 may be visualized the 3D-rotation group of a regular tetrahedron: can you see how each element acts?

Exercises 4.3. Key concepts: *Transposition (representation of elements)* *Odd/even permutations* A_n

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

5 Cosets & Factor Groups

In this chapter we partition a group into subsets in such a way that the *set of subsets* inherits a natural group structure. This is a long and abstract story, though the essentials aren't new; this is precisely what happens with modular arithmetic (itself a generalization of even and odd).

Example 5.1. In $\mathbb{Z}_3 = \{0, 1, 2\}$ the elements are really *subsets* $[0], [1], [2]$ of the *integers* $\mathbb{Z}$: that is,

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

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

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

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

5.1 Cosets & Normal Subgroups

Our main goal is to generalize Example 5.1. Start by observing that the identity element $[0] \in \mathbb{Z}_3$ is in fact a *subgroup* ($3\mathbb{Z}$) of $\mathbb{Z}$ from which the other subsets $[1]$, $[2]$ are obtained by *translation*.

Definition 5.2. Let H be a subgroup of G and $g \in G$. The *left coset* of H containing g is

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

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

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

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

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

Example (5.1 cont). Since $G = \mathbb{Z}$ is written additively, the left and right cosets of $H = [0] = 3\mathbb{Z}$ containing g are written

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

These cosets are precisely the elements of $\mathbb{Z}_3$!

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

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

The last observation is in fact general—the proof is an exercise.

Lemma 5.3. *Every subgroup of an abelian group G is normal.*

A subgroup of a non-abelian group *might* be normal, but is more likely not to be (see Example 5.4.2).

Examples 5.4. 1. The subgroup $H = \langle 2 \rangle = \{0, 2, 4\} \leq \mathbb{Z}_6$ has two distinct cosets (left = right since $\mathbb{Z}_6$ is abelian):

$$\begin{aligned} H &= \{0,2,4\} && (= 2 + H = 4 + H) \\ 1 + H &= \{1,3,5\} && (= 3 + H = 5 + H) \end{aligned}$$

Observe how the cosets **partition** $\mathbb{Z}_6$ into equal-sized subsets.

2. The left and right cosets of the subgroup $H = \{e, \mu_1\} \leq D_3$ are as follows:

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

To verify this, either revisit the multiplication table for D_3 (Example 2.25) or use cycle notation (e.g. Example 4.7). This time the left and right cosets of H are not the same: H is *not* a normal subgroup of D_3. The **partitioning** observation still holds: the left cosets partition D_3 into three equal-sized subsets; the right cosets also partition D_3 into equal-sized (but different) subsets.

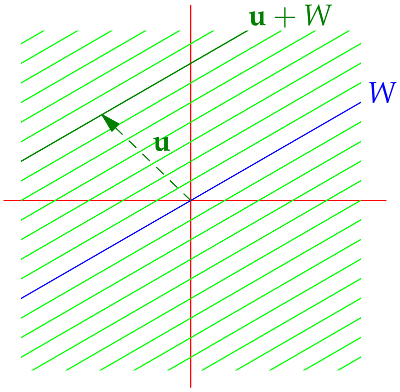
3. Consider a 1-dimensional subspace $W \leq \mathbb{R}^2$. Each coset

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

is a line parallel to W. Once again, the cosets (all lines parallel to W) **partition** $\mathbb{R}^2$.

If this feels too abstract, consider the special case where W is the y-axis: each coset is a vertical line (same x-co-ordinate).

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



4. Consider the alternating group A_n as a subgroup of S_n. Generalizing the argument from Theorem 4.25, we see that for any $\alpha \in A_n$ and $\sigma \in S_n$,

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

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

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

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

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

Theorem 5.5. *Let H be a subgroup of G. Then the left cosets of H partition G. Moreover,*

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

The right cosets also partition G:

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

The blue criterion is often very easy to check. Before reading the proof, convince yourself that each of our previous examples satisfies the result. When H is non-normal, the right cosets partition G differently to the left cosets (e.g. Example 5.4.2).

Example 5.6. This should seem familiar when $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Written additively,

$$a + H = b + H \iff b - a \in H \iff n \mid b - a \iff a \equiv b \pmod{n}$$

The cosets of H are precisely the equivalence classes modulo n. Indeed you've likely encountered the main proof in the context of modular arithmetic.

Proof. We start by verifying the first connective.

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

Now define a relation $\sim$ on G via $x \sim y \iff x^{-1}y \in H$. We claim that this is an equivalence relation:

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

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

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

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

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

The subgroup status of H is precisely what guarantees a partition (compare Theorem 2.14):

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

Symmetry: H satisfies the inverse axiom.

Transitivity: H is closed under the group operation.

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

Example 5.7. The *subset* $H = \{0, 1\} \subseteq \mathbb{Z}_3$ is not a subgroup. Its left 'cosets' fail to partition $\mathbb{Z}_3$:

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

By combining the criteria in Theorem 5.5, we obtain a useful result for identifying when a subgroup is normal *without* explicitly having to compute its cosets. The proof is an exercise.

Corollary 5.8. *Normal subgroups are precisely those which are closed under* ***conjugation****:*

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

Since this holds for all g, we may equivalently observe $g^{-1}hg \in H$.

Exercises 5.1. Key concepts: *left/right cosets & partitioning* *normal subgroup* *kernels are normal*

1. Find the cosets of each subgroup: since the groups are abelian, left and right cosets are equal.

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

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

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

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

   (b) Repeat the question for the subgroup $V := \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ of A_4.

5. Revisit Examples 4.7, particularly its use of cycle notation.

   (a) Find the left and right cosets of $H = \{\rho_0, \delta_1\} \le D_4$. Is H normal?

   (b) Repeat for the subgroup $K = \{\rho_0, \rho_2\}$.

6. Prove Lemma 5.3: every subgroup of an abelian group is normal.

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

   (a) If H has only one element, show that the sets $gH = \{gh : h \in H\}$ do partition G.

   (b) Show that the 'cosets' of $H = \{1,3\}$ also partition $\mathbb{Z}_4$, even though H is not a subgroup.

8. Let $H = \{\sigma \in S_4 : \sigma(4) = 4\}$. Show that H is a subgroup of S_4. Is it *normal*?

9. Prove Corollary 5.8.

10. (a) Suppose $G = H \times K$, $J \triangleleft H$ and let $\widetilde{J} = J \times \{e_K\}$. Prove that $\widetilde{J} \triangleleft G$.
    (*When $J = H$ this is often written $H \triangleleft (H \times K)$. A similar result holds for K.*)

    (b) Explain how Example 5.4.3 fits into part (a).

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

    $$a \sim b \iff \exists h \in H,\ k \in K \text{ such that } a = hbk$$

    (a) Prove that $\sim$ is an equivalence relation on G and describe the elements of the equivalence class of $a \in G$; this is called a *double coset*.

    (b) Compute the double cosets of $H = \{e, (1\,2)\}$ and $K = \{e, (1\,3)\}$ as subgroups of S_3.

5.2 Lagrange's Theorem & Indices

We've been inching towards a powerful result; hopefully you've hypothesized this already!

Theorem 5.9 (Lagrange). *In a finite group, the order of a subgroup divides the order of the group.*[21]

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

Note that the converse is *false*: e.g. A_4 has order 12, but no subgroup of order 6 (Exercise 4.3.7). The argument is merely a generalized version of the proof of Theorem 4.25 ($|A_n| = \frac{1}{2}|S_n|$).

Proof. Suppose $H \le G$ and fix $g \in G$. The function *left-multiplication by g*

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

is a bijection (inverse function $(L_g)^{-1} = L_g^{-1}$). Every left coset of H therefore has the same cardinality as H. Since the left cosets partition G (Theorem 5.5), we conclude that

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

We could instead have used the right coset partition. Here is an example of Lagrange's power.

Corollary 5.10. *Up to isomorphism, there is a unique group of prime order p, namely $\mathbb{Z}_p$.*

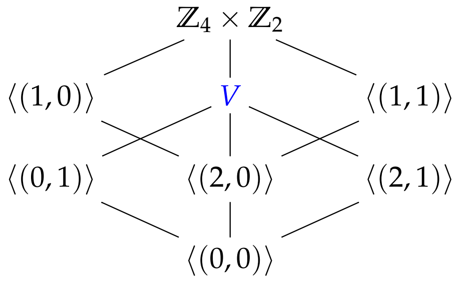
Proof. Suppose G is a group with prime order p. Since $p \ge 2$, we may choose some element $g \ne e$. The order of the cyclic subgroup $\langle g \rangle \le G$ satisfies:

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

We conclude that $|\langle g \rangle| = p$. But then $G = \langle g \rangle$ is cyclic and so isomorphic to $\mathbb{Z}_p$ (Theorem 3.7). $\blacksquare$

Example 5.11. $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ has order 8 so its non-trivial proper subgroups can only have orders 2 or 4 and are thus isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_4$ or V. These can be identified by thinking about all possible generators; V requires three elements of order 2 which we indeed have! Here is the subgroup diagram: all proper subgroups are cyclic except $V = \{(0,0),(2,0),(0,1),(2,1)\}$.

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



[21] This is often misremembered as 'the order of an element divides the order of the group,' which is the special case when H is a *cyclic subgroup* of G. Corollary 3.16 is the even more special case when G is cyclic: $\langle s \rangle \le \mathbb{Z}_n$ has order $\frac{n}{\gcd(s,n)}$.

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

Definition 5.12. The *index* $(G : H)$ of a subgroup $H \leq G$ is the cardinality of the set of (left) cosets:

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

The index is also the cardinality of the set of *right* cosets (Exercise 9). If G is finite, then $(G : H) = \frac{|G|}{|H|}$.

Examples 5.13. 1. If $G = \mathbb{Z}_{20}$ and $H = \langle 2 \rangle = \{0, 2, 4, \ldots, 18\}$, then there are $(G : H) = \frac{20}{10} = \frac{|G|}{|H|} = 2$ cosets (left and right are equal here):

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

2. Recall the orthogonal and special orthogonal groups (Example 2.28 & Exercise 2.2.8):

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

Since every orthogonal matrix has determinant ±1, it feels as if $\mathrm{SO}_n(\mathbb{R})$ should be 'half' of $\mathrm{O}_2(\mathbb{R})$. Since both groups are infinite (indeed uncountable), we need the index to confirm this intuition. Recall Theorem 5.5: given $A, B \in \mathrm{O}_n(\mathbb{R})$,

$$\begin{aligned} A\,\mathrm{SO}_n = B\,\mathrm{SO}_n(\mathbb{R}) &\iff B^{-1}A \in \mathrm{SO}_n(\mathbb{R}) \\ &\iff \det(B^{-1}A) = 1 \\ &\iff \det B = \det A \end{aligned}$$

Since determinant can take only two possible values in $\mathrm{O}_n(\mathbb{R})$, we conclude that there are precisely two cosets $\big(\mathrm{O}_n(\mathbb{R}) : \mathrm{SO}_n(\mathbb{R})\big) = 2$.

3. The integers form an (additive) subgroup of the real numbers $\mathbb{R}$. Observe that

$$x\mathbb{Z} = y\mathbb{Z} \iff y - x \in \mathbb{Z}$$

It follows that there is exactly one coset for every real number in the half-open interval $[0, 1)$; otherwise said, $\psi(x) = x\mathbb{Z}$ defines a bijection of the interval $[0, 1)$ with the set of cosets $\{x\mathbb{Z}\}$. We conclude that there are uncountably many cosets!

Theorem 5.14. *If $K \leq H \leq G$ is a sequence of subgroups, then*

$$(G : K) = (G : H)(H : K)$$

If G is a finite group then the result is essentially trivial:

$$(G : K) = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = (G : H)(H : K)$$

Our proof also covers infinite groups (and even infinite indices, if multiplication of such makes sense to you!). To help understand how it works, first consider a straightforward example.

Example (5.13.1, cont.). If $G=\mathbb{Z}_{20}$, $H=\langle 2\rangle$ and $K=\langle 10\rangle$, then

$$K=\{0,10\}\le H=\{0,2,4,6,8,10,12,14,16,18\}\le G=\{0,1,2,3,\ldots,19\}$$

so we have the required subgroup relationship. Here are the indices and (left) cosets in each case:

- $(G:H)=2$ with cosets H and $1+H$. Each coset has the form g_i+H with either $g_0=0$ or $g_1=1$: these values are *representatives* of the two cosets.
- $(H:K)=\frac{10}{2}=5$ cosets, with representatives $h_0=0$, $h_1=2$, $h_2=4$, $h_3=6$, $h_4=8$:
$$K=\{0,10\},\ \ 2+K=\{2,12\},\ \ 4+K=\{4,14\},\ \ 6+K=\{6,16\},\ \ 8+K=\{8,18\}$$
- $(G:K)=\frac{20}{2}=10=(G:H)(H:K)$. The cosets this time are
$$K=\{0,10\},\quad 1+K=\{1,11\},\quad 2+K=\{2,12\},\quad \ldots,\quad 9+K=\{9,19\}$$
with representatives $0,1,\ldots,9$. The crucial observation for the proof is that representatives are formed by *summing* those above: the cosets of K in G are precisely $(g_i+h_j)+K$.

Proof. Choose an element g_i from each left coset of H in G and an element h_j from each left coset of K in H. Plainly

$$(G:H)=|\{g_i\}|\quad\text{and}\quad(H:K)=\left|\{h_j\}\right|$$

We claim that the left cosets of K in G are precisely the sets $(g_ih_j)K$. Certainly each of these is a coset; we show that these *partition* G, whence the collection $\{(g_ih_j)K\}$ must comprise *all* left cosets.

- Every $g\in G$ lies in some left coset of H, so $\exists g_i\in G$ with $g\in g_iH$.
Now ${g_i}^{-1}g\in H$ lies in some left coset of K in H, so $\exists h_j\in H$ with ${g_i}^{-1}g\in h_jK$.
But then $g\in(g_ih_j)K$, whence every $g\in G$ lies in at least one set $(g_ih_j)K$.
- Suppose $y\in g_ih_jK\cap g_\alpha h_\beta K$. Since $K\le H$ and the left cosets of H partition G, we have
$$y\in g_iH\cap g_\alpha H\implies g_\alpha=g_i$$
But then ${g_i}^{-1}y\in h_jK\cap h_\beta K\implies h_\beta=h_j$ similarly, since the left cosets of K in H partition H. It follows that the sets $(g_ih_j)K$ are disjoint.

Since the left cosets of K in G are given by $\{(g_ih_j)K\}$, it is immediate that

$$(G:K)=\left|\{g_ih_j\}\right|=|\{g_i\}|\left|\{h_j\}\right|=(G:H)(H:K)$$

■

Exercises 5.2. Key concepts: *Lagrange's Theorem* *index of a subgroup (counting cosets)*

1. Find the indices of the following subgroups:

(a) $\langle 9\rangle\le\mathbb{Z}_{12}$ (b) $6\mathbb{Z}\le 2\mathbb{Z}$ (c) $(\mathbb{Q}^+,\cdot)\le(\mathbb{Q}^\times,\cdot)$

2. Let $G = \mathbb{Z}_8$, $H = \langle 2 \rangle = \{0, 2, 4, 6\}$ and $K = \langle 4 \rangle = \{0, 4\}$. Write out all the cosets for the three subgroup relations $K \leq H$, $H \leq G$ and $K \leq G$, and verify the index multiplication formula (Theorem 5.14).

3. Let $G = S_4$ and consider the subgroup tower $K \leq H \leq G$ where

$$K = \{e, (1\,2\,3), (1\,3\,2)\} \cong \mathbb{Z}_3 \quad \text{and} \quad H = \{\sigma \in S_4 : \sigma(4) = 4\} \cong S_3$$

   (a) Write out the elements of the two left cosets $K \leq H$, namely $K = eK$ and $(1\,2)K$ with representatives $h_0 = e$ and $h_1 = (1\,2)$.

   (b) Repeat part (a) for the four cosets of H in $G = S_4$: observe that $g_0 = e$, $g_1 = (1\,4)$, $g_2 = (2\,4)$, $g_3 = (3\,4)$ are representatives.

   (c) Compute the eight left cosets of K in S_4 and verify that they are $(g_i h_j)K$ in accordance with the proof of Theorem 5.14.

4. Let G have order pq where p, q are both prime. Show that every proper subgroup of G is cyclic.

5. Use Lagrange's Theorem to prove that all proper subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$ are cyclic. Hence construct its subgroup diagram.

6. Find the subgroups of $\mathbb{Z}_6 \times \mathbb{Z}_2$ and draw its subgroup diagram.

   (*Hint: At least one proper subgroup is* non-cyclic*!*)

7. Suppose $(G : H) = 2$. Prove that H is a normal subgroup of G.

8. Prove that $\{e\}$ and G are both normal subgroups of G: what are the cosets and the indices in each case?

   (*Remember that G could be infinite!*)

9. For each left coset gH of H in G, choose a representative g_j. Prove that the function

$$\Phi : g_j H \mapsto H g_j^{-1}$$

   is injective from the set of left cosets to the set of right cosets.

   (*With the reverse argument this shows that the sets of left and right cosets have the same cardinality*)

10. Let $G = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

   (a) Prove that G is a group under addition.

   (b) Prove that $H = \{3m + 2n\sqrt{2} : m, n \in \mathbb{Z}\}$ is a subgroup of index six in G.
   (*Hint: what does it mean for $a + b\sqrt{2}$ and $c + d\sqrt{2}$ to lie in the same coset of H?*)

11. We modify Example 5.13.3.

   (a) The sets $\mathbb{Q}$ and $\mathbb{Z}$ are both groups under addition. Show that there is exactly one coset of $\mathbb{Z}$ in $\mathbb{Q}$ for each rational $q \in [0, 1)$. Hence conclude that $(\mathbb{Q} : \mathbb{Z}) = \aleph_0$ is countably infinite.

   (b) Describe the index of U_n (n^{th} roots of unity) as a subgroup of the circle group S^1.

5.3 Factor Groups

Given $H \leq G$, we ask whether the set of left cosets $\{gH : g \in G\}$ has a *natural group structure* inherited from that of G. In our motivating Example (5.1) this is precisely how $\mathbb{Z}_3$ was created from the integers, by 'squashing' all elements of each coset down to a single object. We simply want to do this in general. To see how this might (or might not) work, recall some previous examples.

Examples (5.4, cont). 1. The set of (left) cosets for $H = \langle 2 \rangle = \{0, 2, 4\} \leq \mathbb{Z}_6$ is

$$\{H,\ 1+H\} = \Big\{\{0,2,4\}, \{1,3,5\}\Big\}$$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Addition in $\mathbb{Z}_6$

$\oplus$	H	$1+H$
H	H	$1+H$
$1+H$	$1+H$	H

Addition in $\{H, 1+H\}$

We use addition in $\mathbb{Z}_6$ to define addition of cosets via

$$(a+H) \oplus (b+H) := (a+b) + H$$

This seems nice, though consider the steps of the computation more carefully:

(a) First ***choose** representatives* a and b of the two cosets.

(b) Then *add within the original group* $a + b \in \mathbb{Z}_6$.

(c) Finally, *take the left coset* $(a+b) + H$.

If $\oplus$ is to make sense, the outcome $(a+b)+H$ must be *independent* of the **choices** in step (a). For instance, to properly conclude that $H \oplus (1+H) = 1+H$ we must check *nine* possibilities:

$$a \in \{0,2,4\},\ b \in \{1,3,5\} \implies a+b \in \{1,3,5\} \quad \text{(modulo 6)}$$

To save time, we verify all possibilities simultaneously: If $x \in a+H$ and $y \in b+H$, then

$$(x+y) - (a+b) = (x-a) + (y-b) \in H \implies (x+y) + H = (a+b) + H$$

Addition of cosets $\oplus$ is therefore well-defined. The second table above suggests that the set of cosets forms a group under $\oplus$; indeed $\psi(x) = x + H$ defines an isomorphism of $\mathbb{Z}_2$ with this so-called *factor group*.

2. We repeat the process for the subgroup $H = \{e, \mu_1\} \leq D_3$. The left cosets are

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

As above, we attempt to define the 'natural' operation on the set of left cosets

$$aH \otimes bH := (ab)H \qquad (ab \text{ is composition/multiplication within } D_3)$$

This time there is a serious problem: note that $\rho_1 H = \mu_3 H$, however,

$$\rho_1 H \otimes \rho_1 H = (\rho_1 \rho_1)H = \rho_2 H \qquad \mu_3 H \otimes \mu_3 H = (\mu_3 \mu_3)H = eH = H$$

This is a contradiction: $\rho_2 H \neq H$, but the result of both calculations *should be the same*. The freedom of **choice** (part (a)) in the definition of $\otimes$ leads to different outcomes: the natural operation $\otimes$ *does not exist* (is not well-defined), and thus cannot produce a group structure.

Well-definition of the Factor Group Structure

The examples indicate that only some subgroups $H \leq G$ behave nicely when trying to view the set of left cosets as a group. But which subgroups? To answer this question, we repeat some of our discussion abstractly. Let H be a subgroup of G and define the natural multiplication of left cosets[22]

$$aH \cdot bH := (ab)H \tag{$*$}$$

This is well-defined precisely when

$$xH = aH,\ yH = bH \implies (xy)H = (ab)H \tag{$\dagger$}$$

If the natural multiplication of cosets is well-defined, the fact that $hH = H$ and $gH = gH$ for any $h \in H$, $g \in G$, tells us that

$$(hg)H = gH, \text{ or equivalently } g^{-1}hg \in H \tag{Theorem 5.5}$$

Since this holds *for all* $g \in G$ and $h \in H$, Corollary 5.8 says that ***H* is a normal subgroup of *G*.** Not only is the converse also true, but the resulting structure forms a group under this operation.

Theorem 5.15. *Suppose $H \leq G$ and consider the natural operation $(*)$ on the set of (left) cosets.*

1. *$(*)$ is well-defined if and only if H is a normal subgroup of G.*
2. *In such cases, $(*)$ defines a* group structure *on the set of cosets.*

Since this process only works when H is a normal subgroup, the prefix 'left' is irrelevant.

Definition 5.16. Suppose $H \lhd G$. The group of cosets ${}^{G}\!/_{H} := \{gH : g \in G\}$ (read 'G mod H') under the natural operation $(*)$ is termed a *factor group* (or *quotient group*).

Factor group notation looks like division in part because if G is finite, then $\left|{}^{G}\!/_{H}\right| = (G : H) = \frac{|G|}{|H|}$.

Proof. 1. $(\Rightarrow)$ The above discussion shows that well-definition of $(*)$ implies $H \lhd G$.

$(\Leftarrow)$ Assume $H \lhd G$, and suppose $xH = aH$ and $yH = bH$. By Theorem 5.5, $h := x^{-1}a$ and $\tilde{h} := y^{-1}b$ are both in H. But then,

$$(xy)^{-1}(ab) = y^{-1}(x^{-1}a)b = y^{-1}hb = (y^{-1}hy)\tilde{h}$$

which lies in H by Corollary 5.8 ($y^{-1}hy \in H$). We conclude that $(xy)H = (ab)H$ ($\dagger$).

2. Since the natural operation is well-defined, we need only verify the group axioms for $\left({}^{G}\!/_{H}, \cdot\right)$.

Closure: Given $aH, bH \in {}^{G}\!/_{H}$, we see that $aH \cdot bH = (ab)H$ is also coset.

Associativity: $aH \cdot (bH \cdot cH) = aH \cdot (bc)H = a(bc)H$. Similarly $(aH \cdot bH) \cdot cH = (ab)cH$. By the associativity of $(G, \cdot)$, these cosets are identical.

Identity: The *identity coset* $H = eH$ does the job: $eH \cdot aH = (ea)H = aH = (ae)H = aH \cdot eH$.

Inverse: $a^{-1}H \cdot aH = (a^{-1}a)H = eH = H$, etc., therefore $(aH)^{-1} = a^{-1}H$.

■

[22] Since this operation arises naturally from that on G, we use the same notation (here multiplication).

'Identifying' Factor Groups

The first goal when faced with a factor group ${}^{G}/_{H}$ is often to *identify* it by recognizing some well-understood group to which it is isomorphic. In Section 6.2 we'll develop the main piece of abstract machinery for doing this. Since this upcoming approach can be difficult to apply, it is worth first spending a little time with some basic examples. In particular, we can straightforwardly describe the factor groups of every cyclic group: by Theorem 3.7, we need only do this for $\mathbb{Z}$ and $\mathbb{Z}_n$...

Factor Groups of $\mathbb{Z}$ (modular arithmetic done right) If n is a positive integer, its integer multiples $n\mathbb{Z} = \langle n \rangle$ form a (normal) subgroup of $\mathbb{Z}$. The coset of $n\mathbb{Z}$ containing $x \in \mathbb{Z}$ is plainly

$$x + n\mathbb{Z} = \{x + kn : k \in \mathbb{Z}\} = \big\{y \in \mathbb{Z} : y \equiv x \pmod n\big\}$$

This coset is what we have been calling 'x' in $\mathbb{Z}_n$! This provides the formal definition of $\mathbb{Z}_n$ (superseding Definition 2.16) and trivially demonstrating that $\mathbb{Z}_n$ is an abelian group.

Definition 5.17. Let $n \in \mathbb{N}$. The group $\mathbb{Z}_n$ is the factor group ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$.

We typically drop the repeated $n\mathbb{Z}$ terms when calculating, recovering our familiar notation: e.g.

$$4 + 5 = 2 \in \mathbb{Z}_7 \quad \text{means} \quad (4 + 7\mathbb{Z}) + (5 + 7\mathbb{Z}) = 2 + 7\mathbb{Z} \in {}^{\mathbb{Z}}/_{7\mathbb{Z}}$$

Factor Groups of Finite Cyclic Groups The first example on page 57 shows that ${}^{\mathbb{Z}_6}/_{\langle 2 \rangle} \cong \mathbb{Z}_2$. This generalizes straightforwardly.

Example 5.18. $\langle 5 \rangle = \{0, 5, 10, 15\} \leq \mathbb{Z}_{20}$ has factor group

$${}^{\mathbb{Z}_{20}}/_{\langle 5 \rangle} = \big\{\langle 5 \rangle\,,\ 1 + \langle 5 \rangle\,,\ 2 + \langle 5 \rangle\,,\ 3 + \langle 5 \rangle\,,\ 4 + \langle 5 \rangle\big\}$$

which is isomorphic to $\mathbb{Z}_5$ via the isomorphism

$$\psi : \mathbb{Z}_5 \to {}^{\mathbb{Z}_{20}}/_{\langle 5 \rangle} : x \mapsto x + \langle 5 \rangle$$

Theorem 5.19. *If $d \mid n$, then ${}^{\mathbb{Z}_n}/_{\langle d \rangle} \cong \mathbb{Z}_d$. More generally, ${}^{\mathbb{Z}_n}/_{\langle s \rangle} \cong \mathbb{Z}_{\gcd(s,n)}$.*

Proof. Define $\psi : \mathbb{Z}_d \to {}^{\mathbb{Z}_n}/_{\langle d \rangle} : x \mapsto x + \langle d \rangle$. We prove that this is an isomorphism.

Well-definition/injectivity: For any $x, y \in \mathbb{Z}_d$,

$$\begin{aligned} x = y\ (\in \mathbb{Z}_d) &\iff x - y \in \langle d \rangle \iff x + \langle d \rangle = y + \langle d \rangle \\ &\iff \psi(x) = \psi(y) \end{aligned}$$

Surjectivity: Any coset $x + \langle d \rangle$ (being $\psi(x)$) lies in range(ψ).

Homomorphism: For any $x, y \in \mathbb{Z}_d$,

$$\begin{aligned} \psi(x + y) &= (x + y) + \langle d \rangle = \big(x + \langle d \rangle\big) + \big(y + \langle d \rangle\big) \\ &= \psi(x) + \psi(y) \end{aligned}$$

The general case follows by Corollary 3.16: if $d = \gcd(s, n)$, then $\langle s \rangle = \langle d \rangle$. ■

Further Examples Naïve identification of factor groups often boils down to a two-step hack.

1. Find the order of the factor group ${}^{G}\!/_{H}$ by computing the index $(G:H)$.
2. Determine which group of order $(G:H)$ is correct.

If ${}^{G}\!/_{H}$ is abelian, the Fundamental Theorem (3.26) might supply candidates. Step 2 can often be accomplished by considering orders of elements (cosets). The simple observation can help with this.

Lemma 5.20. *Let ${}^{G}\!/_{H}$ be a factor group. Then $(gH)^m = H \iff g^m \in H$ ($mg \in H$ if G additive). By Corollary 3.9, the* ***order of the element*** *$gH \in {}^{G}\!/_{H}$ is the smallest $m \in \mathbb{N}$ for which $g^m \in H$. Moreover, this number $\min\{m \in \mathbb{N} : g^m \in H\}$ divides the order of g (in G).*

Examples 5.21. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_8$. We identify the factor group ${}^{G}\!/_{H}$ for three subgroups H.

1. The subgroup $H = \langle(0,1)\rangle = \{(0,0),(0,1),\ldots,(0,7)\}$ has 8 elements, so the factor group ${}^{G}\!/_{H}$ has order $\frac{|G|}{|H|} = \frac{4\cdot 8}{8} = 4$. By the Fundamental Theorem, ${}^{G}\!/_{H}$ is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

   We can decide which by considering the orders of elements in ${}^{G}\!/_{H}$:

   $\mathbb{Z}_2 \times \mathbb{Z}_2$: Every element has order at most 2.

   $\mathbb{Z}_4$: There exists a generator with order 4.

   Start playing with elements (cosets)! It doesn't take long to observe that

   $$k(1,0) = (k,0) \in H \iff 4 \mid k \tag{†}$$

   Otherwise said, $(1,0)+H \in {}^{G}\!/_{H}$ has order 4: we conclude that ${}^{G}\!/_{H} \cong \mathbb{Z}_4$. Since $(1,0)+H$ is a generator, this approach provides an explicit isomorphism $\psi : \mathbb{Z}_4 \cong {}^{G}\!/_{H}$:

   $$\psi(x) = (x,0) + H \qquad \Big(= \{(x,0),(x,1),\ldots,(x,7)\}\Big)$$

2. The subgroup $H = \langle(0,2)\rangle = \{(0,0),(0,2),(0,4),(0,6)\}$ has 4 elements, so $\left|{}^{G}\!/_{H}\right| = \frac{32}{4} = 8$. The factor group is isomorphic to one of $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

   - Exactly as in (†), $(1,0)+H \in {}^{G}\!/_{H}$ has order 4. This rules out $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ as a candidate.
   - $\mathbb{Z}_8$ is ruled out since every $(x,y)+H$ has order at most 4: for any (x,y),

     $$4(x,y) = (4x,4y) = (0,4y) = 2y(0,2) \in H$$

   By process of elimination, we conclude that ${}^{G}\!/_{H} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

3. The subgroup $H = \langle(2,4)\rangle = \{(0,0),(2,4)\}$ produces a factor group of order $\left|{}^{G}\!/_{H}\right| = \frac{32}{2} = 16$, so we must consider *five* non-isomorphic possibilities:

   $$\mathbb{Z}_{16}, \quad \mathbb{Z}_2 \times \mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

   - The coset $(0,1)+H \in {}^{G}\!/_{H}$ has order 8, since

     $$k\big((0,1)+H\big) = H \iff (0,k) \in H \iff 8 \mid k$$

   - Every $(x,y)+H$ has order dividing 8, since

     $$8(x,y) = (8x,8y) = (0,0) \in H$$

   The only candidate satisfying both properties is $\mathbb{Z}_2 \times \mathbb{Z}_8$.

For factor groups of infinite or non-abelian groups, more creative strategies might be required.

Examples 5.22. 1. As seen in Exercise 5.2.7, every index-2 subgroup $H \leq G$ is normal. Since there is only one group of order 2 up to isomorphism, in such a case ${}^{G}\!/_{H} \cong \mathbb{Z}_2$.

For instance, $R_n \lhd D_n$ has index $(D_n : R_n) = 2$. The two cosets are,

$$\begin{aligned} &\text{Rotations:} && R_n = \{\rho_0, \ldots, \rho_{n-1}\} \\ &\text{Reflections:} && \mu R_n = \{\mu_1, \ldots, \mu_n\}, \text{ where } \mu \text{ is any reflection.} \end{aligned}$$

$\circ$	R_n	μR_n
R_n	R_n	μR_n
μR_n	μR_n	R_n

The Cayley table for the factor group ${}^{D_n}\!/_{R_n} = \{R_n, \mu R_n\}$ is shown. Consider how the calculation $(\mu R_n)(\mu R_n) = R_n$ says that the composition of two reflections is a rotation!

2. In Exercise 5.1.4, we saw that the alternating group A_4 has the Klein four-group identified as

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

as a normal subgroup. Since the factor group has order $(A_4 : V) = \frac{12}{4} = 3$ and there is only one group of order 3 up to isomorphism, we conclude that ${}^{A_4}\!/_{V} \cong \mathbb{Z}_3$.

3. (Example 5.4.3, simplified) Given $W = \{(0, y) : y \in \mathbb{R}\} \leq \mathbb{R}^2$, each coset (vertical line)

$$\{(x, y) : y \in \mathbb{R}\} \quad (= (x, 0) + W)$$

intersects the x-axis at a unique point $(x, 0)$. Otherwise said, we have a bijection,

$$\psi : \mathbb{R} \to {}^{\mathbb{R}^2}\!/_{W} : x \mapsto (x, 0) + W$$

This is moreover an isomorphism, since

$$\psi(x_1 + x_2) = (x_1 + x_2) + W = (x_1 + W) + (x_2 + W) = \psi(x_1) + \psi(x_2)$$

4. (Hard) Let $G = \mathbb{Z} \times \mathbb{Z}_4$ and consider the subgroup

$$H = \langle (2, 1) \rangle = \{\ldots, (-4, 2), (-2, 3), (0, 0), (2, 1), (4, 2), (6, 3), (8, 0), (10, 1), \ldots\}$$

We cannot count cosets using the index formula. Instead we find a simple representative of each coset:

$$\begin{aligned} &\text{If } x = 2n \text{ is even:} && (x, y) + H = (2n, y) + H = (0, y - n) + H \\ &\text{If } x = 2n + 1 \text{ is odd:} && (x, y) + H = (2n + 1, y) + H = (1, y - n) + H \end{aligned}$$

In any coset, there is a *unique representative* either of the form $(0, z)$ or $(1, z)$, where $z \in \mathbb{Z}_4$: it follows that there are 8 cosets. To finish things off, observe that

$$k(1, 0) = (k, 0) \in H \iff 8 \mid k$$

whence $(1, 0) + H \in {}^{G}\!/_{H}$ has order 8: we conclude that ${}^{G}\!/_{H} \cong \mathbb{Z}_8$.

We'll see more examples, and revisit others, in Section 6.2 once we've developed more machinery.

Exercises 5.3. Key concepts:

Factor group $\quad {}^{G}\!/_{H}$ *a group* $\iff H \lhd G \qquad \mathbb{Z}_n := {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \qquad$ *identifying* ${}^{G}\!/_{H}$

1. List the cosets of the subgroup $H = \langle 3 \rangle$ in $G = \mathbb{Z}_{15}$. By mimicking the proof of Theorem 5.19, show that $\psi : \mathbb{Z}_3 \mapsto {}^{G}\!/_{H} : x \mapsto x + H$ is a well-defined isomorphism.

2. (Exercise 5.1.2 cont.) If $H = \{(0,0),(0,2),(2,0),(2,2)\}$, identify the factor group ${}^{\mathbb{Z}_4 \times \mathbb{Z}_4}\!/_{H}$.

3. Identify the factor group ${}^{G}\!/_{H}$ where $H = \langle (2,4) \rangle \le G = \mathbb{Z}_4 \times \mathbb{Z}_6$.

4. Let $G = \mathbb{Z}_9 \times \mathbb{Z}_9$.

   (a) State the elements of the subgroup $H = \langle (3,6) \rangle$. Now identify ${}^{G}\!/_{H}$ by showing that every element of the factor group has order at most 9 and that it contains an element of order 9.

   (b) Repeat with $H = \langle 3 \rangle \times \langle 6 \rangle$ (*this isn't a trick question*).

5. Let G be any group. To what groups are ${}^{G}\!/_{\{e\}}$ and ${}^{G}\!/_{G}$ isomorphic?

6. (a) If G is abelian and $H \le G$, prove that ${}^{G}\!/_{H}$ is abelian.

   (b) If ${}^{G}\!/_{H}$ is abelian, can we conclude that G and/or H is abelian? Explain.

7. (a) Let G be a cyclic group with subgroup H. Prove that ${}^{G}\!/_{H}$ is cyclic.

   (b) If ${}^{G}\!/_{H}$ is cyclic, does it follow that G is cyclic? Explain.

8. (Exercise 5.2.10, cont.) The factor group ${}^{G}\!/_{H}$ is abelian and of order 6, whence it is cyclic. Prove this explicitly by finding a generator and thus an isomorphism $\psi : \mathbb{Z}_6 \to {}^{G}\!/_{H}$.

9. (Example 5.22.2, cont.) Find an explicit isomorphism $\psi : \mathbb{Z}_3 \cong {}^{A_4}\!/_{V}$.

10. Exercise 5.1.5 showed that $\{\rho_0, \rho_2\}$ is a normal subgroup of D_4. To what well-known group is the factor group ${}^{D_4}\!/_{\{\rho_0,\rho_2\}}$ isomorphic? Prove your assertion.

11. If $H \lhd G$ has index $(G : H) = 2$, then the factor group ${}^{G}\!/_{H}$ is necessarily isomorphic to $\mathbb{Z}_2$.

    (a) Prove that $\psi : \mathbb{Z}_2 \to {}^{S_n}\!/_{A_n}$ defined by $\psi(x) = (1\,2)^x A_n$ is an isomorphism.

    (b) Find an explicit isomorphism $\psi : \mathbb{Z}_2 \to {}^{O_n(\mathbb{R})}\!/_{SO_n(\mathbb{R})}$.

12. (Exercise 5.1.10, cont.) Suppose $G = H \times K$, $J \lhd H$ and $\widehat{J} = J \times \{e_K\}$. Prove that ${}^{G}\!/_{\widetilde{J}} = {}^{H}\!/_{J} \times K$. Can you quickly verify Examples 5.21.1, 2, and 5.22.3 in this language?

13. Complete the proof of Lemma 5.20 by showing that the order of the element/coset $gH \in {}^{G}\!/_{H}$ divides the order of the element $g \in G$.

    (*Hint: Use the division algorithm similarly to the proof of Theorem 3.12*)

14. (Hard) Let $H = \langle (2,3) \rangle \le G = \mathbb{Z}_5 \times \mathbb{Z}$. Prove that ${}^{G}\!/_{H} \cong \mathbb{Z}_{15}$.

15. (Hard!!) If $G = \mathbb{Z}_{10} \times \mathbb{Z}_6 \times \mathbb{Z}$ and $H = \langle (4,2,3) \rangle$, identify ${}^{G}\!/_{H}$ as a direct product $\mathbb{Z}_m \times \mathbb{Z}_n$.

    (*Hint: show that exactly one representative of the coset $(x,y,z) + H$ has $z = 0, 1$ or 2*)

6 Homomorphisms & The First Isomorphism Theorem

The main goal of this chapter is to discuss the link between homomorphisms, normal subgroups and factor groups. The key result is the subject of Section 6.2: the First Isomorphism Theorem.

6.1 Kernels, Images and Normal Subgroups

In Section 2.5 we established several important facts that are worth refreshing and summarizing here.

Definition 6.1. The *kernel* and *image* of a homomorphism[23] $\phi : G \to L$ are the sets

$$\ker\phi = \{g \in G : \phi(g) = e\}, \qquad \operatorname{Im}\phi = \{\phi(g) : g \in G\}$$

Lemma 6.2. *Suppose $\phi : G \to L$ is a homomorphism.*

1. *(Exercise 2.5.11c) ϕ maps identity to identity and inverse to inverse:*

$$\phi(e_G) = \phi(e_L) \quad \text{and} \quad \forall g \in G,\ \big(\phi(g)\big)^{-1} = \phi(g^{-1})$$

2. *(Exercise 2.5.12) $\ker\phi$ is a subgroup of G and $\operatorname{Im}\phi$ is a subgroup of L.*

Do these exercises now, even if you did them earlier!

Examples 6.3. 1. The function $\phi(x) = 2x \pmod 4$ defines a homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_4$ with

$$\ker\phi = \{x \in \mathbb{Z} : 2x \equiv 0 \pmod 4\} = 2\mathbb{Z}, \qquad \operatorname{Im}\phi = \{0, 2\}$$

Plainly $\ker\phi$ is a subgroup of $\mathbb{Z}$ and $\operatorname{Im}\phi$ is a subgroup of $\mathbb{Z}_4$.

2. Every linear map $\mathrm{T} : V \to W$ between vector spaces is a homomorphism. In linear algebra its kernel is better known as its *nullspace*

$$\ker\mathrm{T} = \mathcal{N}(\mathrm{T}) = \{\mathbf{v} \in V : \mathrm{T}(\mathbf{v}) = \mathbf{0}\}$$

If $\mathrm{T} = \mathrm{L}_A : \mathbb{R}^n \to \mathbb{R}^m$ is left-multiplication by a matrix A, then $\operatorname{Im}\mathrm{T}$ is the *column space* of A.

Since the groups in these examples are abelian, all subgroups are automatically normal. In fact the kernel of *every* homomorphism is a normal subgroup, though the same cannot be said for images.

Lemma 6.4. *If $\phi : G \to L$ is a homomorphism, then $\ker\phi \lhd G$.*

Proof. The kernel is a subgroup by part 2 of Lemma 6.2, so we need only check normality. For this we appeal to the conjugation criterion (Corollary 5.8). If $g \in G$ and $k \in \ker\phi$, then

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_L \implies gkg^{-1} \in \ker\phi$$

Note how the first equality used the homomorphism property and part 1 of the Lemma. ∎

[23] All homomorphisms in this chapter (indeed outside of Section 2.5) are between *groups*.

Examples 6.5. 1. (Recall Exercises 2.4.8a & 2.5.1g) We've seen that $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism. We therefore obtain a normal subgroup

$$\ker\det = \{A \in \mathrm{GL}_n(\mathbb{R}) : \det A = 1\} \lhd \mathrm{GL}_n(\mathbb{R})$$

Otherwise said, $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$.

2. (Example 5.4.2, cont.) $\phi : \mathbb{Z}_2 \to D_3$ defined by $\phi(x) = \mu_1^x$ is a homomorphism. Certainly $\ker\phi = \{0\} \lhd \mathbb{Z}_2$, however $\operatorname{Im}\phi = \{e, \mu_1\}$ is not a *normal* subgroup of S_3.

Kernels, Images and Describing Homomorphisms

Since every kernel is a normal subgroup, it makes sense to ask how its cosets may be counted and distinguished.

Lemma 6.6. *Let $\phi : G \to L$ be a homomorphism. There is precisely one coset of $\ker\phi$ for each element of $\operatorname{Im}\phi$:*

$$g_1 \ker\phi = g_2 \ker\phi \iff \phi(g_1) = \phi(g_2)$$

Otherwise said, the index *equals the order of the image:* $(G : \ker\phi) = |\operatorname{Im}\phi|$.

The proof is an abstraction of Example 5.13.2 (where $\phi = \det : \mathrm{O}_2(\mathbb{R}) \to \mathbb{R}^\times$).

Proof. For all $g_1, g_2 \in G$, we have

$$\begin{aligned} g_1\ker\phi = g_2\ker\phi &\iff g_2^{-1}g_1 \in \ker\phi && \text{(Theorem 5.5)}\\ &\iff \phi(g_2^{-1}g_1) = e_L && \text{(Definition of } \ker\phi)\\ &\iff \phi(g_2)^{-1}\phi(g_1) = e_L && \text{(Homomorphism properties)}\\ &\iff \phi(g_1) = \phi(g_2) \end{aligned}$$

■

The Lemma is really part of the upcoming punchline in Section 6.2. For the moment we apply it to help describe and count homomorphisms.

Theorem 6.7. *Let $\phi : G \to L$ be a homomorphism. If G is finite, then $\operatorname{Im}\phi$ is a finite group whose order divides that of G. The same holds for L. Otherwise said,*

$$|G| < \infty \implies |\operatorname{Im}\phi| \,\Big|\, |G| \quad \textit{and} \quad |L| < \infty \implies |\operatorname{Im}\phi| \,\Big|\, |L|$$

If both groups are finite, then $|\operatorname{Im}\phi| \,\Big|\, \gcd(|G|, |L|)$.

Proof. If G is a finite group, then $\ker\phi \le G$ is finite. Apply Lemma 6.6 to see that

$$|\operatorname{Im}\phi| = (G : \ker\phi) = \frac{|G|}{|\ker\phi|}$$

is a divisor of $|G|$. The second situation $|\operatorname{Im}\phi| \,\Big|\, |L|$ is Lagrange's Theorem (5.9).

■

Examples 6.8. 1. If $\phi : G \to L$ is a homomorphism and $\gcd\big(|G|, |L|\big) = 1$, then we have $|\operatorname{Im}\phi| = 1$. The image is necessarily the *trivial subgroup* $\operatorname{Im}\phi = \{e_L\}$ and there is exactly one homomorphism, namely the *trivial homomorphism* ($\forall g \in G,\ \phi(g) = e_L$).

2. Consider all homomorphisms $\phi : \mathbb{Z}_4 \to S_3$. Since the domain is cyclic, describing $\phi(1)$ is enough to obtain $\phi(x) = \big(\phi(1)\big)^x$. Since $\gcd(|\mathbb{Z}_4|, |S_3|) = 2$, we have $|\operatorname{Im}\phi| = 1$ or 2. Either:

   - $\operatorname{Im}\phi = \{e\}$ and we obtain the trivial homomorphism $\phi_0(x) = e$.
   - $\operatorname{Im}\phi$ is a subgroup of order 2, of which S_3 has exactly three: $\{e, (2\,3)\}$, $\{e, (1\,3)\}$, $\{e, (1\,2)\}$. This results in three further homomorphisms (for a total of four)

$$\phi_1(x) = (2\,3)^x, \qquad \phi_2(x) = (1\,3)^x, \qquad \phi_3(x) = (1\,2)^x$$

We now turn to the general question of homomorphisms between finite cyclic groups $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$. Two facts make this relatively simple:

1. As above, choosing $\phi(1)$ defines the homomorphism: $\phi(x) = \phi(1) + \cdots + \phi(1) = \phi(1) \cdot x$.
2. $|\operatorname{Im}\phi|$ must divide $d = \gcd(m, n)$. Since $\mathbb{Z}_n$ has exactly one subgroup of each order dividing n (Corollary 3.16), $\operatorname{Im}\phi$ must be a subgroup of the *unique* subgroup $\left\langle \frac{n}{d} \right\rangle \leq \mathbb{Z}_n$ of order d:

$$\operatorname{Im}\phi \leq \left\langle \frac{n}{d} \right\rangle = \left\{0, \frac{n}{d}, \frac{2n}{d}, \ldots, \frac{(d-1)n}{d}\right\}$$

   It is enough to see what happens if we let $\phi(1)$ be each element of this subgroup in turn...

Corollary 6.9. *There are $d = \gcd(m, n)$ distinct homomorphisms $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$, namely*

$$\phi_k(x) = \frac{kn}{d}x \quad \text{where} \quad k = 0, \ldots, d-1$$

Proof. We check that each ϕ_k is well-defined; the calculation uses the fact that $\frac{m}{d}$ is an *integer.*

$$\begin{aligned} x = y \in \mathbb{Z}_m &\implies y = x + \lambda m \text{ for some } m \in \mathbb{Z} \\ &\implies \phi_k(y) = \phi_k(x + \lambda m) = \frac{kn}{d}(x + \lambda m) = \frac{kn}{d}x + \lambda k \frac{m}{d} n = \frac{kn}{d}x \qquad (\text{in } \mathbb{Z}_n) \\ &\qquad\quad = \phi_k(x) \end{aligned}$$

By observation 1, each ϕ_k is a homomorphism. Observation 2 says there are no other candidates. ∎

Example 6.10. We describe all homomorphisms $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{20}$.
Since $\gcd(12, 20) = 4$, we see that $\operatorname{Im}\phi \leq \langle 5 \rangle = \{0, 5, 10, 15\} \leq \mathbb{Z}_{20}$. There are four choices:

$$\phi_0(x) = 0, \qquad \phi_1(x) = 5x, \qquad \phi_2(x) = 10x, \qquad \phi_3(x) = 15x \pmod{20}$$

We similarly see that there are four distinct homomorphisms $\psi : \mathbb{Z}_{20} \to \mathbb{Z}_{12}$:

$$\psi_0(x) = 0, \qquad \psi_1(x) = 3x, \qquad \psi_2(x) = 6x, \qquad \psi_3(x) = 9x \pmod{12}$$

Most of these examples rely on the domain of a homomorphism being cyclic (observation 1). It is typically much harder to find and describe homomorphisms when the domain is non-cyclic.

Exercises 6.1. Key concepts: $(G : \ker\phi) = |\mathrm{Im}\,\phi| \quad |\mathrm{Im}\,\phi| \,\Big|\, \gcd\big(|G|, |L|\big)$

1. Check that you have a homomorphism (use Corollary 6.9) and compute its kernel and image.

   (a) $\phi : \mathbb{Z}_8 \to \mathbb{Z}_{14}$ defined by $\phi(x) = 7x \pmod{14}$.

   (b) $\phi : \mathbb{Z}_{36} \to \mathbb{Z}_{20}$ defined by $\phi(x) = 5x \pmod{20}$.

2. Describe all homomorphisms between the groups:

   (a) $\phi : \mathbb{Z}_{15} \to \mathbb{Z}_{80}$ (b) $\phi : \mathbb{Z} \to \mathbb{Z}_3$

   (c) $\phi : \mathbb{Z}_6 \to D_4$ (d) $\phi : \mathbb{Z}_{15} \to A_4$

3. State a linear map $\mathrm{T} : \mathbb{R}^2 \to \mathbb{R}^2$ whose kernel is the y-axis (a normal subgroup of $\mathbb{R}^2$). What type of linear map is the function T?

4. Find the kernel and image of each homomorphism and verify that $\ker\phi$ is normal:

   (a) The *trace* of a matrix $\mathrm{tr} : M_2(\mathbb{R}) \to \mathbb{R} : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto a + d$.

   (b) $\mathrm{T} : \mathbb{R}^3 \to \mathbb{R}^4 : \mathbf{x} \mapsto \begin{pmatrix} 1 & 1 & -1 \\ 0 & 3 & -1 \\ 1 & 4 & -2 \\ 2 & 5 & -3 \end{pmatrix} \mathbf{x}$

5. Explain why the map ϕ is a homomorphism and find $\ker\phi$:

$$\phi : S_n \to \big(\{1, -1\}, \cdot\big) : \sigma \mapsto \begin{cases} 1 & \text{if } \sigma \text{ even} \\ -1 & \text{if } \sigma \text{ odd} \end{cases}$$

6. Suppose $\phi : G \to L$ is a homomorphism, and that $H \le G$ and $K \le L$ are subgroups.

   (a) Prove that $\phi(H) := \{\phi(h) : h \in H\}$ is a subgroup of $\mathrm{Im}\,\phi$.

   (b) Give an example to show that $\mathrm{Im}\,\phi$ need not be a normal subgroup of L.

   (c) Prove that the *inverse image* $\phi^{-1}(K) = \{g \in G : \phi(g) \in K\}$ is a subgroup of G.

7. (Exercise 3.2.6, cont.) Prove that the number of distinct *isomorphisms* $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ equals the order of the multiplicative group of units $(\mathbb{Z}_n^\times, \cdot_n)$.

8. (a) Suppose $\phi : \mathbb{Z}_{(m)} \times \mathbb{Z}_{(n)} \to L$ is a well-defined homomorphism.[24] Prove that $\phi(x, y) = ax + by$, where $a = \phi(1, 0)$ and $b = \phi(0, 1)$.

   (b) Prove that $\phi : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n$ is a well-defined homomorphism if and only if there exist integers a, b, c, d for which

$$\phi(x, y) = \big(ax + by, cx + dy\big), \quad m \mid bn \quad \text{and} \quad n \mid cm$$

9. Find all homomorphisms $\phi : \mathbb{Z}_2 \times \mathbb{Z}_7 \to \mathbb{Z}_2 \times \mathbb{Z}_5$. How do you know that there are no more?

10. Consider $\phi : D_4 \to D_4 : \sigma \mapsto \sigma^2$. Explain why ϕ is *not* a homomorphism.

[24] As in Theorem 3.7, $\mathbb{Z}_{(m)}$ is a generic additive cyclic group: either $\mathbb{Z}$ or $\mathbb{Z}_m$.

6.2 The First Isomorphism Theorem

Lemma 6.4 says that every kernel is a normal subgroup. In fact *all* normal subgroups arise this way.

Theorem 6.11 (Canonical Homomorphism). *Let G be a group and $H \lhd G$. The function*

$$\gamma : G \to {}^{G}\!/_{H} \quad \textit{defined by} \quad \gamma(g) = gH$$

is a homomorphism with $\ker \gamma = H$.

Proof. Since H is normal, ${}^{G}\!/_{H}$ is a factor group. By the definition of multiplication in ${}^{G}\!/_{H}$,

$$\gamma(g_1)\gamma(g_2) = g_1H \cdot g_2H = (g_1g_2)H = \gamma(g_1g_2)$$

whence γ is a group homomorphism. Moreover, the identity in the factor group is H, whence

$$g \in \ker \gamma \iff \gamma(g) = H \iff g \in H$$

■

This might feel a little sneaky, and we'd have preferred a codomain that wasn't a factor group! Our hope is vain however, for the next result—arguably the most important in elementary group theory—shows that **every homomorphism with the same kernel is essentially γ in disguise.**

Theorem 6.12 (1st Isomorphism). *Let $\phi : G \to L$ be a homomorphism with kernel H. Then*

$$\mu : {}^{G}\!/_{H} \to \operatorname{Im}\phi \quad \textit{defined by} \quad \mu(gH) = \phi(g)$$

is an isomorphism. Otherwise said: $\phi = \mu \circ \gamma$ and ${}^{G}\!/_{\ker\phi} \cong \operatorname{Im}\phi$.

A *commutative diagram* provides a helpful summary: $\phi = \mu \circ \gamma$ means we get the same result by following arrows from G to $\operatorname{Im}\phi$ regardless of the path.

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "\gamma"'] & & \operatorname{Im}\phi \\
& {}^{G}\!/_{\ker\phi} \arrow[ur, "\mu"'] &
\end{tikzcd}$$

The 1st isomorphism theorem has analogues in several other parts of mathematics: at the very least you should have met its close kin from linear algebra, the rank–nullity theorem.

Proof. The factor group exists since $\ker\phi \lhd G$ (Lemma 6.4). We check the isomorphism properties:

Well-definition and Bijectivity: These are immediate after writing $H = \ker\phi$:

$$g_1H = g_2H \overset{\text{Lemma}}{\underset{6.6}{\iff}} \phi(g_1) = \phi(g_2) \iff \mu(g_1H) = \mu(g_2H)$$

Homomorphism: For all $g_1H, g_2H \in {}^{G}\!/_{H}$,

$$\begin{aligned}
\mu(g_1H \cdot g_2H) &= \mu(g_1g_2H) = \phi(g_1g_2) && \text{(coset multiplication \& definition of } \mu\text{)} \\
&= \phi(g_1)\phi(g_2) && (\phi \text{ is a homomorphism}) \\
&= \mu(g_1H)\mu(g_2H)
\end{aligned}$$

■

Examples 6.13. 1. Let $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{20}$ be the homomorphism $\phi(x) = 5x \pmod{20}$ (Example 6.10). Its kernel and image are

$$\begin{aligned} &\ker\phi = \big\{x \in \mathbb{Z}_{12} : 5x \equiv 0 \pmod{20}\big\} = \{0,4,8\} = \langle 4\rangle \le \mathbb{Z}_{12} \\ &\operatorname{Im}\phi = \{5x \in \mathbb{Z}_{20} : x \in \mathbb{Z}_{12}\} = \{0,5,10,15\} = \langle 5\rangle \le \mathbb{Z}_{20} \end{aligned}$$

The relevant factor group is

$$\mathbb{Z}_{12}/_{\ker\phi} = \Big\{\{0,4,8\},\{1,5,9\},\{2,6,10\},\{3,7,11\}\Big\} = \{\langle 4\rangle, 1+\langle 4\rangle, 2+\langle 4\rangle, 3+\langle 4\rangle\}$$

The canonical homomorphism γ and the isomorphism μ are

$$\begin{aligned} &\gamma(x) = x + \langle 4\rangle \\ &\mu\big(x+\langle 4\rangle\big) = 5x \end{aligned}$$

$$\begin{tikzcd} \mathbb{Z}_{12} \arrow[r, "\gamma"'] \arrow[rr, bend left, "\phi"] & \mathbb{Z}_{12}/_{\langle 4\rangle} \arrow[r, "\mu"'] & \operatorname{Im}\phi \\ x \arrow[r, mapsto] & x+\langle 4\rangle \arrow[r, mapsto] & 5x \end{tikzcd}$$

2. The homomorphism $\phi : \mathbb{R} \to (\mathbb{C}^\times, \cdot) : x \mapsto e^{2\pi i x}$ has

$$\ker\phi = \big\{x \in \mathbb{R} : e^{2\pi i x} = 1\big\} = \mathbb{Z} \quad \text{and} \quad \operatorname{Im}\phi = S^1 \qquad (S^1 \text{ is the circle group})$$

The canonical homomorphism γ and the isomorphism μ from the theorem are

$$\gamma : \mathbb{R} \to \mathbb{R}/_{\mathbb{Z}} : x \mapsto x + \mathbb{Z} \quad \text{and} \quad \mu : \mathbb{R}/_{\mathbb{Z}} \to S^1 : x + \mathbb{Z} \mapsto e^{2\pi i x}$$

Think about how this relates to Example 5.13.3.

3. The homomorphism $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (x,y) \mapsto 3x - 2y$ satisfies

$$\phi(x,y) = (0,0) \iff 3x = 2y \iff (x,y) = (2n,3n) \text{ for some } n \in \mathbb{Z}$$

We conclude that $\ker\phi = \langle(2,3)\rangle$. The canonical homomorphism is therefore

$$\gamma : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}/_{\langle(2,3)\rangle} : (x,y) \mapsto (x,y) + \langle(2,3)\rangle$$

Since $n = \phi(n,n)$, the homomorphism is surjective: $\operatorname{Im}\phi = \mathbb{Z}$. By the 1st isomorphism theorem,

$$\mathbb{Z}\times\mathbb{Z}/_{\langle(2,3)\rangle} \cong \mathbb{Z} \quad \text{via} \quad \mu\big((x,y) + \langle(2,3)\rangle\big) = 3x - 2y$$

4. $\phi(x,y) = (x, y-x)$ is a well-defined homomorphism $\phi : \mathbb{Z} \times \mathbb{Z}_6 \to \mathbb{Z}_3 \times \mathbb{Z}_6$. Moreover,

$$\phi(x,y) = (0,0) \iff \begin{cases} x = 3k, \text{ and} \\ y = x = 3k \in \mathbb{Z}_6 \end{cases}$$

whence $\quad \ker\phi = \langle(3,3)\rangle = \{\ldots,(-6,0),(-3,3),(0,0),(3,3),(6,0),\ldots\}$

Moreover, ϕ is surjective: e.g. $(m,n) = \phi(m, n+m)$. We conclude that

$$\mathbb{Z}\times\mathbb{Z}_6/_{\langle(3,3)\rangle} \cong \mathbb{Z}_3 \times \mathbb{Z}_6 \quad \text{via} \quad \mu\big((x,y) + \langle(3,3)\rangle\big) = (x, y-x)$$

Identifying Factor Groups (revisited)

The 1st isomorphism theorem may be applied to the identification of factor groups. Given $H \triangleleft G$, we cook up a homomorphism $\phi : G \to L$ with $\ker \phi = H$ and conclude that ${}^{G}/_{H} \cong \operatorname{Im} \phi$. This typically requires some creativity: there are many options, and both L and a formula for ϕ need to be found simultaneously! We first revisit some examples from the previous section in this context.

Examples (5.21, mk.II). For each subgroup H of $G = \mathbb{Z}_4 \times \mathbb{Z}_8$, we hunt for a suitable homomorphism with $\ker \phi = H$.

1. Given $H = \langle (0,1) \rangle$, we need a homomorphism for which $\phi(0,1)$ is the identity. This is very simple: just ignore y! Define

   $$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_4 : (x,y) \mapsto x$$

   This indeed has kernel $\ker \phi = \{(0,y) : y \in \mathbb{Z}_8\} = H$. By the 1st isomorphism theorem,

   $${}^{G}/_{H} \cong \operatorname{Im} \phi = \mathbb{Z}_4$$

   via the isomorphism $\mu\big((x,y)+H\big) = x$. Note that $(x,y)+H = (x,0)+H$, whence μ is the *inverse* of the isomorphism $\psi : x \mapsto (x,0)+H$ stated previously!

2. Given $H = \langle (0,2) \rangle$ we require $\phi(0,2)$ to be the identity. This may be achieved by taking y modulo 2 and defining

   $$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_4 \times \mathbb{Z}_2 : (x,y) \mapsto (x,y)$$

   This is well-defined

   $$\phi(x+4m, y+8n) = (x+4m, y+8n) = (x,y) = \phi(x,y) \qquad \text{(since } 2 \mid 8)$$

   and a homomorphism with required kernel H. Moreover, ϕ is surjective, whence

   $${}^{G}/_{H} \cong \operatorname{Im} \phi = \mathbb{Z}_4 \times \mathbb{Z}_2$$

   via the isomorphism $\mu\big((x,y)+H\big) = (x,y)$. Once again μ is the inverse of $\psi(x,y) = (x,y)+H$ in the original example.

3. Finding a homomorphism with kernel $H = \langle (2,4) \rangle = \big\{(0,0),(2,4)\big\}$ is somewhat trickier. One approach is to observe that

   $$(x,y) \in H \iff x \equiv 0 \pmod 2 \text{ and } y - 2x \equiv 0 \pmod 8$$

   This suggests

   $$\phi : \mathbb{Z}_4 \times \mathbb{Z}_8 \to \mathbb{Z}_2 \times \mathbb{Z}_8 : (x,y) \mapsto \big(x, y-2x\big)$$

   It is worth checking that this is well-defined: the $2x$ in the second co-ordinate is crucial! Certainly ϕ has the correct kernel. It is moreover surjective: $(m,n) = \phi(m, n+2m)$. In conclusion,

   $${}^{G}/_{H} \cong \operatorname{Im} \phi = \mathbb{Z}_2 \times \mathbb{Z}_8$$

   via the isomorphism $\mu\big((x,y)+H\big) = (x, y-2x)$.

Examples 6.14. Two final examples follow a similar theme, though with infinite groups. We'll generalize these in Exercise 10.

1. We identify the factor group ${}^{G}\!/_{H} = {}^{\mathbb{Z}\times\mathbb{Z}}\!/_{\langle(1,-1)\rangle}$.

   We require a homomorphism where $(1,-1) \in \ker\phi$. An obvious candidate is

   $$\phi : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z} : (x,y) \mapsto x+y$$

   Certainly $(x,y) \in \ker\phi \iff x+y=0 \iff y=-x \iff (x,y) \in \langle(1,-1)\rangle$. Moreover, $x = \phi(x,0)$ for any $x \in \mathbb{Z}$, so this is a surjective homomorphism. We conclude that

   $${}^{\mathbb{Z}\times\mathbb{Z}}\!/_{\langle(1,-1)\rangle} \cong \operatorname{Im}\phi = \mathbb{Z}$$

2. We identify the factor group ${}^{G}\!/_{H} = {}^{\mathbb{Z}\times\mathbb{Z}}\!/_{\langle(4,6)\rangle}$.

   It is tempting to try a homomorphism $\psi(x,y) = 6x-4y$ or $\psi(x,y) = 3x-2y$. These certainly satisfy $\psi(4,6) = 0$, but they also have $\psi(2,3) = 0$ which we don't want!

   As a hint for how to proceed, note that the element/coset $(2,3)+H \in {}^{G}\!/_{H}$ has order 2:

   $$2(2,3) = (4,6) \in H$$

   We'd therefore like a homomorphism that maps $(2,3)$ to an element of order 2: the simple function $\xi : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}_2 : (x,y) \mapsto y-x$ certainly does this! We try combining these functions:

   $$\phi : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}_2 : (x,y) \mapsto (3x-2y, y-x)$$

   Let's compute the kernel:

   $$\phi(3x-2y, y-x) = (0,0) \implies 3x = 2y \in \mathbb{Z} \implies (x,y) = (2m,3m) : m \in \mathbb{Z}$$

   Substitute this into the second factor: $y-x = m = 0 \in \mathbb{Z}_2 \implies m = 2n$ is even, from which $(x,y) = (4n,6n)$. It is trivially verified that all such pairs lie in the kernel, whence $\ker\phi = \langle(4,6)\rangle$, as required. Finally,

   $$\phi(1,1) = (1,0), \quad \phi(2,3) = (0,1) \implies (u,v) = \phi(u+2v, u+3v)$$

   says that ϕ is surjective. We conclude that ${}^{G}\!/_{H} \cong \mathbb{Z}\times\mathbb{Z}_2$.

Exercises 6.2. Key concepts:

Canonical homomorphism $\gamma : G \to {}^{G}\!/_{H}$ $\quad$ 1^{st} *isomorphism theorem* $\mu : {}^{G}\!/_{\ker\phi} \cong \operatorname{Im}\phi$

1. Let $\phi : \mathbb{Z}_{18} \to \mathbb{Z}_{12}$ be the homomorphism $\phi(x) = 10x$.

   (a) Find the kernel of and image of ϕ.

   (b) List the elements of the factor group ${}^{\mathbb{Z}_{18}}\!/_{\ker\phi}$.

   (c) State an explicit isomorphism $\mu : {}^{\mathbb{Z}_{18}}\!/_{\ker\phi} \to \operatorname{Im}\phi$.

   (d) To what basic group $\mathbb{Z}_n$ is the factor group isomorphic?

2. Repeat the previous question for the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_{20} : x \mapsto 8x$.

3. For each function $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, find the kernel and identify the factor group $\mathbb{Z} \times \mathbb{Z}/_{\ker \phi}$.

   (a) $\phi(x, y) = 3x + y$ (b) $\phi(x, y) = 2x - 4y$

4. (a) If a subgroup H of $G = \mathbb{Z}_{15} \times \mathbb{Z}_3$ has order 5, find its elements.
   (b) Show that $\phi(x, y) = (x, y)$ is a homomorphism $\phi : G \to \mathbb{Z}_3 \times \mathbb{Z}_3$ with $\ker \phi = H$.
   (c) What does the 1st isomorphism theorem tell us about the factor group $G/_H$?

5. Suppose G is a finite group with normal subgroup H and that $\phi : G \to L$ is a homomorphism with $\ker \phi = H$. Prove that $(G : H) \leq |L|$ with equality if and only if ϕ is surjective.

6. Consider the map $\phi : \mathbb{Z} \times \mathbb{Z}_{12} \to \mathbb{Z}_3 \times \mathbb{Z}_6$ defined by

$$\phi(x, y) = \big(2x + y, y\big)$$

   (a) Verify that ϕ is a well-defined homomorphism.
   (b) Compute $\ker \phi$ and identify the factor group $\mathbb{Z} \times \mathbb{Z}_{12}/_{\ker \phi}$

7. Let $H = \langle(3, 1)\rangle \leq G = \mathbb{Z}_9 \times \mathbb{Z}_3$. Find an explicit homomorphism $\phi : G \to \mathbb{Z}_9$ whose kernel is H, and thus identify the factor group $G/_H$.
   (*Hint:* $(x, y) \in H = \{(0, 0), (3, 1), (6, 2)\} \iff \ldots$)

8. Consider $H = \langle(3, 3)\rangle \leq G = \mathbb{Z}_9 \times \mathbb{Z}_9$. Find a surjective homomorphism $\phi : G \to \mathbb{Z}_3 \times \mathbb{Z}_9$ whose kernel is H and hence prove that $G/_H \cong \mathbb{Z}_3 \times \mathbb{Z}_9$.

9. Let $\phi : S^1 \to S^1 : z \mapsto z^2$.

   (a) Find the kernel of ϕ and describe the canonical homomorphism $\gamma : S_1 \to S^1/_{\ker \phi}$.
   (b) What does the first isomorphism theorem say about the factor group $S^1/_{\ker \phi}$.
   (c) For each n, identify the factor group $S^1/_{U_n}$, where U_n is the group of n^{th} roots of unity.

10. We identify $G/_H = \mathbb{Z} \times \mathbb{Z}/_{\langle(a,b)\rangle}$. Suppose $d = \gcd(a, b)$ where a, b are not both zero.

   (a) Let $\psi(x, y) = \frac{b}{d}x - \frac{a}{d}y$ be the homomorphism $\psi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. Find $\ker \psi$.
   (b) Show that $G/_H$ contains an element of order d, namely $(\frac{a}{d}, \frac{b}{d}) + H$.
   (c) Bézout's identity says $\exists \kappa, \lambda \in \mathbb{Z}$ for which $\kappa a + \lambda b = d$. The function

$$\xi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_d : (x, y) \mapsto \kappa x + \lambda y$$

   plainly maps $(\frac{a}{d}, \frac{b}{d})$ to the generator $1 \in \mathbb{Z}_d$. Compute $\ker \phi$ for the combined map

$$\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_d : (x, y) \mapsto \left(\frac{b}{d}x - \frac{a}{d}y, \kappa x + \lambda y\right)$$

   (d) Identify the factor group $\mathbb{Z} \times \mathbb{Z}/_{\langle(a,b)\rangle}$.
   (e) Find an explicit isomorphism $\mu : \mathbb{Z} \times \mathbb{Z}/_{\langle(21,35)\rangle} \to \mathbb{Z} \times \mathbb{Z}_7$.

6.3 Conjugation, Cycle Types, Centers and Automorphisms

In this section we consider an important type of homomorphism and some its consequences.

Definition 6.15. Let G be a group and $x, y \in G$. We say that y is *conjugate to* x if

$$\exists g \in G \quad \text{such that} \quad y = gxg^{-1}$$

If $g \in G$ is fixed, then *conjugation by* g is the map $c_g : G \to G : x \mapsto gxg^{-1}$.

We've met this notion before: recall that a subgroup H is normal if and only if $c_g(h) \in H$ for all $g \in G$ (Corollary 5.8). It should also be familiar from linear algebra, in the context of *similarity.* Recall that square matrices A, B are similar if $B = MAM^{-1}$ for some invertible M. Such matrices have the same eigenvalues and, essentially, 'do the same thing' with respect to different bases. An explicit group theory analogue of this is Theorem 6.19 below.

Lemma 6.16. *Conjugation by g is a isomorphism $c_g : G \cong G$.*

Proof. Conjugation by g^{-1} is the inverse function of c_g^{-1}:

$$c_{g^{-1}}(c_g(x)) = g^{-1}gxg^{-1}(g^{-1})^{-1} = x, \quad \text{etc.}$$

We moreover have a homomorphism:

$$c_g(xy) = g(xy)g^{-1} = \left(gxg^{-1}\right)\left(gyg^{-1}\right) = c_g(x)c_g(y)$$

■

Lemma 6.17. *Conjugacy is an equivalence relation ($x \sim y \iff \exists g \in G$ such that $y = gxg^{-1}$).*

The proof is an exercise. The equivalence classes under conjugacy are termed *conjugacy classes.*

Examples 6.18. 1. If G is abelian then every conjugacy class contains only one element:

$$x \sim y \iff \exists g \in G \quad \text{such that} \quad y = gxg^{-1} = xgg^{-1} = x$$

2. The smallest non-abelian group is S_3 has conjugacy classes

$$\{e\}, \quad \{(1\,2), (1\,3), (2\,3)\}, \quad \{(1\,2\,3), (1\,3\,2)\}$$

This can be computed directly, but it follows immediately from…

Theorem 6.19. *The conjugacy classes of S_n are the* cycle types*: elements are conjugate if and only if they have the same cycle-type.*

If an element $\sigma \in S_n$ is written as a product of disjoint cycles, then its cycle-type is clear. For instance:

- $(1\,2\,3)(4\,5)$ has the same cycle-type as $(1\,5\,6)(2\,3)$: we might call these 3,2-cycles.
- $(1\,2)(3\,4)$ has cycle-type 2,2.

Before seeing a proof it is beneficial to try an example.

Example 6.20. If $\rho = (2\,4\,3)$ and $\sigma = (1\,2)(3\,4)$ in S_4, then

$$\rho\sigma\rho^{-1} = (2\,4\,3)(1\,2)(3\,4)(2\,3\,4) = (1\,4)(2\,3)$$

This plainly has the same cycle-type as σ. Moreover, it may be obtained by applying ρ to the entries of σ!

$$\rho\sigma\rho^{-1} = (1\,4)(2\,3) = \big(\rho(1)\,\rho(2)\big)\big(\rho(3)\,\rho(4)\big) \tag{$*$}$$

This tells us how to reverse the process: given 2,2-cycles $\sigma = (1\,2)(3\,4)$ and $\tau = (1\,4)(2\,3)$ simply place σ on top of τ in a table to define a suitable $\rho = (2\,4\,3)$ for which $\rho\sigma\rho^{-1} = \tau$.

x	1	2	3	4
$\rho(x)$	1	4	2	3

The proof is a notational horror, but it amounts to nothing more than the example done abstractly: our goal is to recognize $\rho\sigma\rho^{-1}$ in exactly the form $(*)$, taking ρ of each entry in each cycle.

Proof. ($\Rightarrow$) First consider conjugation of a k-cycle $\sigma = (a_1 \cdots a_k)$ by $\rho \in S_n$. We claim that

$$\rho\sigma\rho^{-1} = \big(\rho(a_1)\cdots\rho(a_k)\big)$$

is **also a k-cycle.** Since this is an equality of functions, we verify by evaluating on all elements of $X = \{1, 2, \ldots, n\}$. There are two cases, which correspond to partitioning $X = A \cup (X \setminus A)$ where $A = \{a_1, \ldots, a_k\}$. First observe that ρ bijectively maps $A \to A$ and $X \setminus A \to X \setminus A$.

1. Suppose $x \in A$. Since $A = \rho(A)$, we may uniquely write $x = \rho(a_j)$. But then

   $$\rho\sigma\rho^{-1}(x) = \rho\sigma\rho^{-1}\big(\rho(a_j)\big) = \rho\sigma(a_j) = \rho(a_{j+1})$$

   where a_{k+1} is understood to equal a_1.
2. Suppose $x \notin A$. We know that $\rho^{-1}(x) \notin A$ is unmoved by σ, whence

   $$\rho\sigma\rho^{-1}(x) = \rho\sigma(\rho^{-1}(x)) = \rho\rho^{-1}(x) = x$$

We conclude that $\rho\sigma\rho^{-1} = \big(\rho(a_1)\cdots\rho(a_k)\big)$ is as claimed. More generally, if $\sigma = \sigma_1 \cdots \sigma_l$ is a product of disjoint cycles, then

$$\rho\sigma\rho^{-1} = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1})\cdots(\rho\sigma_l\rho^{-1})$$

has the same cycle-type as σ.

($\Leftarrow$) Suppose $\sigma = \sigma_1 \cdots \sigma_l$ and $\tau = \tau_1 \cdots \tau_l \in S_n$ have the same cycle-type, written so that corresponding orbits have the same length. Assume we've all single-element orbits are included so that $\bigcup \sigma_i = \{1, \ldots, n\} = \bigcup \tau_i$. Define $\rho \in S_n$ by writing the orbits of σ and τ on top each other

x	σ_1	σ_2	$\cdots$	σ_l
$\rho(x)$	τ_1	τ_2	$\cdots$	τ_l

Since the orbits of σ, & τ partition $X = \{1, \ldots, n\}$, this is plainly defines a permutation. Finally, if $s_{i,j}$ and $t_{i,j}$ are the j^{th} elements of the orbits σ_i and τ_i, then

$$\rho\sigma\rho^{-1}(t_{i,j}) = \rho\sigma(s_{i,j}) = \rho\big(s_{i,j+1}\big) = t_{i,j+1} = \tau\big(t_{i,j}\big)$$

We conclude that $\rho\sigma\rho^{-1} = \tau$, as required. ■

Examples 6.21. 1. The permutations $\sigma = (1\,4\,5)(2\,7\,6)$ and $\tau = (1\,6\,5)(3\,4\,7)$ in S_7 have the same cycle-type and are thus conjugate. The table defines a suitable ρ.

$$\begin{array}{c||ccc|ccc|c} x & 1 & 4 & 5 & 2 & 7 & 6 & 3 \\ \hline \rho(x) & 1 & 6 & 5 & 3 & 4 & 7 & 2 \end{array} \implies \rho = (2\,3)(4\,6\,7)$$

It is worth making a sanity check:

$$\rho\sigma\rho^{-1} = (2\,3)(4\,6\,7)(1\,4\,5)(2\,7\,6)(2\,3)(4\,7\,6) = (1\,6\,5)(3\,4\,7) = \tau$$

Other choices of ρ are available: just write the orbits of σ, τ in different orders. Can you figure out *how many* distinct choice of ρ will work?

2. (Example 5.3.2) We checked previously that $V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a normal subgroup of A_4. Since V contains the identity and all 2,2-cycles it is closed under conjugacy and thus a normal subgroup of both A_4 and S_4.

Automorphisms

We've already seen that conjugation $c_g : G \to G$ by a fixed element $g \in G$ is an isomorphism. We now consider all such maps.

Definition 6.22. An *automorphism* of a group G is an isomorphism of G with itself. The set of such is denoted $\operatorname{Aut} G$. The *inner automorphisms* are the conjugations

$$\operatorname{Inn} G = \{c_g : G \to G \text{ where } c_g(x) = gxg^{-1}\}$$

Example 6.23. There are four homomorphisms $\phi_k : \mathbb{Z}_4 \to \mathbb{Z}_4$ (Corollary 6.9);

$$\phi_0(x) = 0, \quad \phi_1(x) = x, \quad \phi_2(x) = 2x, \quad \phi_3(x) = 3x$$

of which two are automorphisms: $\operatorname{Aut} \mathbb{Z}_4 = \{\phi_1, \phi_3\}$. Observe that ϕ_1 is the identity function and that $\phi_3 \circ \phi_3 = \phi_1$. The automorphisms therefore comprise a *group* (isomorphic to $\mathbb{Z}_2$) under composition of functions.

As for conjugations, since $\mathbb{Z}_4$ is abelian these are uninteresting:

$$g, x \in \mathbb{Z}_4 \implies c_g(x) = g + x + (-g) = x \implies c_g = \phi_1$$

There is only one inner automorphism of $\mathbb{Z}_4$, namely the identity function ϕ_1. This indeed holds in general: if G is abelian, then $\operatorname{Inn}(G) \cong \mathbb{Z}_1$ is trivial.

In general, hunting for automorphisms is difficult. Here is a simple observation that helps to narrow things down. The proof is an exercise.

Lemma 6.24. *If $\phi \in \operatorname{Aut} G$ and $x \in G$, then the orders of x and $\phi(x)$ are identical.*

This helps to streamline the previous example: $\phi(1)$ must have the same order (four) as 1 and so our only possibilities are $\phi(1) = 1$ or $\phi(1) = 3$. These generate the two observed automorphisms.

Example 6.25. We describe all automorphisms ϕ of S_3. Consider $\sigma = (1\,2)$ and $\tau = (1\,2\,3)$. Since the order of an element is preserved by ϕ, we conclude that

$$\phi(e) = e, \quad \phi(\sigma) \in \{(1\,2), (1\,3), (2\,3)\}, \quad \phi(\tau) \in \{(1\,2\,3), (1\,3\,2)\}$$

We therefore have a maximum of *six* possible automorphisms; it is tedious to check, but *all* in fact define automorphisms! Indeed all are conjugations, from which $\operatorname{Aut} S_3 = \operatorname{Inn} S_3$. Here is the data; verify some of it for yourself:

element g	$c_g(e)$	$c_g(1\,2)$	$c_g(1\,3)$	$c_g(2\,3)$	$c_g(1\,2\,3)$	$c_g(1\,3\,2)$
e	e	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,2)$	e	$(1\,2)$	$(2\,3)$	$(1\,3)$	$(1\,3\,2)$	$(1\,2\,3)$
$(1\,3)$	e	$(2\,3)$	$(1\,3)$	$(1\,2)$	$(1\,3\,2)$	$(1\,2\,3)$
$(2\,3)$	e	$(1\,3)$	$(1\,2)$	$(2\,3)$	$(1\,3\,2)$	$(1\,2\,3)$
$(1\,2\,3)$	e	$(2\,3)$	$(1\,2)$	$(1\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,3\,2)$	e	$(1\,3)$	$(2\,3)$	$(1\,2)$	$(1\,2\,3)$	$(1\,3\,2)$

As the next result shows, the automorphisms always form a group under composition; in this case $\operatorname{Aut} S_3$ is a group of order 6 which is easily seen to be *non-abelian*,

$$c_{(1\,2)}c_{(1\,3)} = c_{(1\,3\,2)} \neq c_{(1\,2\,3)} = c_{(1\,3)}c_{(1\,2)}$$

By process of elimination, we conclude that $\operatorname{Aut} S_3 \cong S_3$.

Theorem 6.26. *$\operatorname{Aut} G$ and $\operatorname{Inn} G$ are groups under composition. Moreover $\operatorname{Inn} G \lhd \operatorname{Aut} G$.*

Proof. That $\operatorname{Aut} G$ is a group is simply the fact that composition and inverses of isomorphisms are isomorphisms: you should already have made this argument when answering Exercise 2.5.15. By Lemma 6.16, every conjugation is an isomorphism, and it is simple to check that $c_g \circ c_h = c_{gh}$ and $c_g^{-1} = c_{g^{-1}}$. We conclude that $\operatorname{Inn} G \leq \operatorname{Aut} G$.

For normality, we check that $\operatorname{Inn} G$ is itself closed under conjugation! Let $\tau \in \operatorname{Aut} G$ and $c_g \in \operatorname{Inn} G$. For any $x \in G$, we have[25]

$$\begin{aligned}
(\tau c_g \tau^{-1})(x) &= \tau\Big(c_g\big(\tau^{-1}(x)\big)\Big) \\
&= \tau\Big(g\big(\tau^{-1}(x)\big)g^{-1}\Big) && \text{(definition of } c_g\text{)} \\
&= \Big(\tau(g)\Big)\Big(\tau\big(\tau^{-1}(x)\big)\Big)\Big(\tau(g^{-1})\Big) && \text{(since } \tau \text{ is a homomorphism)} \\
&= \big(\tau(g)\big)x\big(\tau(g)\big)^{-1} && \text{(again since } \tau \text{ is an homomorphism)} \\
&= c_{\tau(g)}(x)
\end{aligned}$$

We conclude that $\tau c_g \tau^{-1} = c_{\tau(g)} \in \operatorname{Inn} G$, from which $\operatorname{Inn} G \lhd \operatorname{Aut} G$. ∎

[25] The challenge in reading the proof is keeping track of where everything lives. To help, the inverse symbol is colored: τ^{-1} (in red) means the inverse *function*, whereas g^{-1} (in blue) means the inverse of an *element* in G.

Centers

We say that an element $g \in G$ *commutes* with another element $x \in G$ if the order of multiplication is irrelevant: $gx = xg$. Otherwise said, g conjugates x to itself: $c_g(x) = x$. It natural to ask whether there are any elements which commute with *all others*. There are two very simple cases:

- If G is abelian, then every element commutes with everything!
- The identity e commutes with everything, regardless of G.

In general, the set of such elements falls somewhere between these extremes. This subset will turn out to be yet another normal subgroup of G.

Definition 6.27. The *center* of a group G is the subset of G which commutes with everything in G:

$$Z(G) := \{g \in G : \forall h \in G,\ gh = hg\}$$

We will prove that $Z(G) \triangleleft G$ shortly. First we give a few examples; unless G is abelian, the center is typically difficult to compute, so we omit more of the details.

Examples 6.28. 1. $Z(G) = G \iff G$ is abelian.

2. $Z(S_n) = \{e\}$ if $n \geq 3$. This is Exercise 4.1.12.

3. $Z(D_{2n+1}) = \{e\}$ and $Z(D_{2n}) = \{e, \rho_{n/2}\}$, where $\rho_{n/2}$ is rotation by 180°. Part of this is in Exercise 12: more generally, this follows from Exercise 4.1.13.

4. $Z\big(\mathrm{GL}_n(\mathbb{R})\big) = \{\lambda I_n : \lambda \in \mathbb{R}^\times\}$. If you've done enough linear algebra to be familiar with eigenvectors, an argument is reasonably straightforward (Exercise 11)

Theorem 6.29. *Let G be any group. Then:*

1. $Z(G) \triangleleft G$ *2.* ${}^{G}/_{Z(G)} \cong \operatorname{Inn} G$

Proof. Everything follows from defining a suitable homomorphism with the correct kernel!

Define $\phi : G \to \operatorname{Inn} G$ by $\phi(g) = c_g$. This is indeed a homomorphism ($\phi(gh) = \phi(g)\phi(h)$):

$$\begin{aligned}\big(\phi(gh)\big)(x) &= c_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = c_g(c_h(x))\\ &= \big(\phi(g)\phi(h)\big)(x)\end{aligned}$$

Now observe that

$$\begin{aligned} g \in \ker\phi &\iff \forall x \in G,\ c_g(x) = gxg^{-1} = x\\ &\iff g \in Z(G)\end{aligned}$$

By Lemma 6.4, $\ker\phi = Z(G)$ is a normal subgroup of G.
To finish, observe that ϕ is surjective (definition of $\operatorname{Inn} G$). The 1st isomorphism theorem tells us that

$${}^{G}/_{Z(G)} \cong \operatorname{Im}\phi = \operatorname{Inn} G$$

■

Exercises 6.3. Key concepts: *Conjugation* *Conjugacy Classes* *Cycle Types are Conjugacy Classes (S_n)* *(Inner) Automorphism* *Center of a Group*

1. Either find some $\rho \in G$ such that $\rho\sigma\rho^{-1} = \tau$, or explain why no such element exists:
   (a) $\sigma = (1\,2\,3),\ \tau = (1\,3\,2)$ where $G = S_3$.
   (b) $\sigma = (1\,4\,5\,6)(2\,3)(5\,6),\ \tau = (1\,2\,3\,4)(5\,6)(2\,6)$ where $G = S_6$.
   (c) $\sigma = (1\,4\,5\,6)(2\,3)(5\,6),\ \tau = (1\,2)(3\,5\,6)$ where $G = S_6$.
2. Recall Example 6.21.1. Find another element $\nu \neq \rho$ for which $\nu\sigma\nu^{-1} = \tau$. Now determine *how many* distinct such ν exist: that is, how many ways can we conjugate σ to get τ?
3. Prove Lemma 6.17. Prove that the relation

   $$x \sim y \iff y \text{ is conjugate to } x$$

   is an equivalence relation on any group G.
4. (a) Suppose y is conjugate to x in a group G. Prove that the orders of x and y are identical.
   (b) Show that the converse to part (a) is *false* by exhibiting two non-conjugate elements of the same order in some group.
5. Let $H \leq G$, fix $a \in G$ and define the *conjugate subgroup* $K = c_a(H) = \{aha^{-1} : h \in H\}$.
   (a) Prove that K is indeed a subgroup of G.
   (b) Prove that the function $\psi : H \to K : h \mapsto aha^{-1}$ is an isomorphism of groups.
   (c) If $H \triangleleft G$, what can you say about $c_a(H)$?
   (d) Let $H = \{e, (1\,2)\} \leq S_3$ and $a = (1\,2\,3)$. Compute the conjugate subgroup $K = c_a(H)$.
6. In Example 6.21.2 we saw that $V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \triangleleft S_4$.
   (a) Show that *normal subgroup* is not transitive by giving an example of a normal subgroup $K \triangleleft V$ which is *not normal* in S_4.
   (b) How many *other* subgroups does S_4 have which are isomorphic to V? Why are none of them normal in S_4?
   (c) Explain why ${}^{S_4}\!/_{V}$ is a group of order six. Prove that

   $$(1\,2)V(1\,3)V \neq (1\,3)V(1\,2)V$$

   Hence conclude that ${}^{S_4}\!/_{V} \cong S_3$.
   (d) Why is it obvious that the following six left cosets are distinct.

   $$V,\ (1\,2)V,\ (1\,3)V,\ (2\,3)V,\ (1\,2\,3)V,\ (1\,3\,2)V$$

   (*Hint: Think about how none of the representatives a of the above cosets move the number 4 and consider* $aV = bV \iff b^{-1}a \in V \ldots$)
   (e) Define an isomorphism $\mu : {}^{S_4}\!/_{V} \to S_3$ and prove that it is an isomorphism.

7. Prove Lemma 6.24: if $\phi \in \operatorname{Aut} G$ and $x \in G$, then $\phi(x)$ has the same order as x.

8. Describe all automorphisms of the Klein four-group V.
   (*Hint: use the previous question!*)

9. Recall Exercise 6.1.7. Explain why $\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^\times$.
   (*Hint: consider* $\phi_k(x) = kx$ *where* $\gcd(k, n) = 1$ *and map* $\psi : k \mapsto \phi_k$)

10. Let G be a group. Prove directly that $Z(G) \lhd G$, *without* using Theorem 6.29. That is:
    (a) Prove that $Z(G)$ is closed under the group operation and inverses.
    (b) Prove that $gZ(G) = Z(G)g$ for all $g \in G$.

11. We identify the center of the general linear group.

    The $n \times n$ matrix $A = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & & & 0 \\ 0 & 0 & 0 & & & 0 \\ \vdots & & & \ddots & \ddots & \\ 0 & 0 & 0 & & 0 & 1 \\ 0 & 0 & 0 & \cdots & & 0 \end{pmatrix}$ has a single one-dimensional eigenspace: $A\mathbf{e}_1 = \mathbf{0}$.

    (a) Let $B \in Z\big(\mathrm{GL}_n(\mathbb{R})\big)$. Use the fact that $AB = BA$ to prove that $B\mathbf{e}_1 = \lambda\mathbf{e}_1$ for some $\lambda \neq 0$.
    (b) Let $\mathbf{x} \in \mathbb{R}^n$ be non-zero and X an invertible matrix for which $X\mathbf{e}_1 = \mathbf{x}$ (i.e. $\mathbf{x}$ is the 1st column of X). Prove that $B\mathbf{x} = \lambda\mathbf{x}$.
    (c) Since the observation in part (b) holds for *any* $\mathbf{x} \in \mathbb{R}^n$, what can we conclude about B? What is the group $Z\big(\mathrm{GL}_n(\mathbb{R})\big)$?

12. (a) Prove that D_4 has center $Z(D_4) = \{e, \rho_2\}$, where ρ_2 is rotation by 180°.
    (b) State the cosets of $Z(D_4)$. What is the order of each? Determine whether ${}^{D_4}\!/_{Z(D_4)}$ is isomorphic to $\mathbb{Z}_4$ or to the Klein four-group V.
    (c) (Hard) Can you find a homomorphism $\phi : D_4 \to D_4$ whose kernel is $Z(D_4)$?
    (*Hint: draw a picture and think about doubling angles of rotation and reflection!*)

13. The *centralizer* of an element $x \in G$ is the set of elements which conjugate x to itself:

    $$C(x) = \{g \in G : gxg^{-1} = x\}$$

    (a) Prove directly that $C(x)$ is a subgroup of G.
    (b) We compute a few centralizers directly. The centralizer of $\sigma = (1\,2\,3) \in S_3$ is the set of all ρ for which

    $$(1\,2\,3) = \rho\sigma\rho^{-1} = \big(\rho(1)\,\rho(2)\,\rho(3)\big)$$

    Otherwise said, ρ must permute the elements $\{1, 2, 3\}$ *in order.* We conclude that

    $$C(\sigma) = \{e, (1\,2\,3), (1\,3\,2)\} = \{e, \sigma, \sigma^2\} \cong \mathbb{Z}_3$$

    In similar fashion, compute the centralizers of the following elements and identify the group $C(\sigma)$:

    i. $\sigma = (1\,2) \in S_4$
    ii. $\sigma = (1\,2\,3\,4\,5)$ in both S_5 and A_5.
    iii. $\sigma = (1\,2)(3\,4)$ in both S_4 and A_4.

14. Prove that if ${}^{G}\!/_{Z(G)}$ is cyclic, then G is abelian. What is the group ${}^{G}\!/_{Z(G)}$ in such a situation?

7 Group Actions

7.1 Group Actions, Fixed Sets and Isotropy Subgroups

You may feel by now that groups are worthy of study purely in their own right—if so great! For many, however, the fundamental reason to care about groups is because of how they *transform sets.* Recall how the symmetric group S_n (Section 4) was defined in terms of what its elements do to the set $\{1, \ldots, n\}$. This is an example of a general situation.

Definition 7.1. An *action*[26] of a group G on a set X is a function $\cdot : G \times X \to X$ for which,

(a) $\forall x \in X,\ e \cdot x = x$, and,

(b) $\forall x \in X,\ g, h \in G,\ g \cdot (h \cdot x) = (gh) \cdot x$.

Part (b) says $g \mapsto g\cdot$ is a homomorphism of *binary structures* $(G, \cdot) \to (\{f : X \to X\}, \circ)$.

Examples 7.2. 1. The symmetric S_n group acts on $X = \{1, 2, \ldots, n\}$. As a sanity check:

   (a) $e(x) = x$ for all $x \in \{1, \ldots, n\}$.

   (b) $\sigma(\tau(x)) = (\sigma\tau)(x)$ is simply composition of functions!

2. If X is the set of orientations of a regular n-gon centered at the origin and with one vertex at $(1, 0)$, then D_n acts on X by rotations and reflections. This is essentially our definition of D_n!

3. Any group G acts on itself by left multiplication ($X = G$). This is essentially the proof of Cayley's Theorem (4.8). G also acts on itself by conjugation ($c_g \circ c_h = c_{gh}$ is Theorem 6.26).

4. Matrix groups act on vector spaces by matrix multiplication. For example the orthogonal group $\mathrm{O}_2(\mathbb{R})$ transforms vectors via rotations and reflections:

$$\mathrm{O}_2(\mathbb{R}) \times \mathbb{R}^2 \to \mathbb{R}^2 : (A, \mathbf{v}) \mapsto A\mathbf{v}$$

5. A group can act on many different sets. Here are three further actions of the orthogonal group:

   i. $\mathrm{O}_2(\mathbb{R})$ acts on $X = \{1, -1\}$ via $A \cdot x := (\det A)x$.

   ii. $\mathrm{O}_2(\mathbb{R})$ acts on $X = \mathbb{R}^3$ via $A \cdot \mathbf{v} := A(v_1\mathbf{i} + v_2\mathbf{j}) + v_3\mathbf{k}$.

   iii. $\mathrm{O}_2(\mathbb{R})$ acts on the unit circle $X = S^1 \subseteq \mathbb{R}^2$ via matrix multiplication $A \cdot \mathbf{v} := A\mathbf{v}$.

We often use actions to help visualize a group (or even define it!); in this context, some actions are better than others. Consider the three actions of $\mathrm{O}_2(\mathbb{R})$ in part 5 above.

i. $X = \{1, -1\}$ is too small to provide a detailed picture of the group since many matrices act in the same way: e.g. $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ both "multiply by 1 (= det A)".

ii. $X = \mathbb{R}^3$ is unnecessarily large. The action leaves any vertical vector untouched.

iii. $X = S^1$ is large enough that the action of distinct matrices can be distinguished without being inefficiently large (a *Goldilocks* action, perhaps?).

[26] This is strictly a *left* action. There is an analogous definition of a *right action.* In these notes, all actions will be left.

These notions can be formalized.

Definition 7.3. Let $G \times X \to X$ be an action.

1. The *fixed set* of $g \in G$ is the set (subset of X)
$$\mathrm{Fix}(g) := \{x \in X : g \cdot x = x\} \qquad \text{(also written } X_g\text{)}$$
2. The *isotropy subgroup* or *stabilizer* of $x \in X$ is the set (subset of G)
$$\mathrm{Stab}(x) := \{g \in G : g \cdot x = x\} \qquad \text{(also written } G_x\text{)}$$
3. The action is *faithful* (or *effective*) if the only element of G fixing everything is e. Equivalently:

   (a) $\mathrm{Fix}(g) = X \iff g = e$ (b) $\bigcap_{x \in X} \mathrm{Stab}(x) = \{e\}$
4. The action is *transitive* if any element of X may be transformed to any other:
$$\forall x, y \in X,\ \exists g \in G \text{ such that } y = g \cdot x$$

Very loosely, an action that is both faithful and transitive is likely reasonable for visualizing a group.

Examples (7.2 cont). 1. The action of S_n on $\{1, 2, \ldots, n\}$ is both faithful and transitive:

Faithful: if $\sigma(x) = x$ for all $x \in \{1, 2, \ldots, n\}$, then $\sigma = e$.

Transitive: if $x \neq y$, then the 2-cycle $(x\,y)$ maps $x \mapsto y$.

2. D_n acts faithfully and transitively on the orientations of the n-gon.
3. The action of a group on itself by left multiplication is both faithful and transitive. Conjugation is more complex: in this context, the stabilizer of $x \in G$ is called its *centralizer* $C(x) = \mathrm{Stab}(x)$.
4. The action of $\mathrm{O}_2(\mathbb{R})$ on $\mathbb{R}^2$ is faithful but not transitive: for instance the zero vector cannot be transformed into any other vector so $\mathrm{Stab}(\mathbf{0}) = \mathrm{O}_2(\mathbb{R})$.
5. We leave these as exercises.

Lemma 7.4. *For each $x \in X$, the stabilizer* $\mathrm{Stab}(x)$ *is indeed a subgroup of G.*

Proof. We use the subgroup criterion:

Non-emptiness Part (a) of Definition 7.1 says that $e \in \mathrm{Stab}(x)$.

Closure This is part (b) of the Definition. Let $g, h \in \mathrm{Stab}(x)$, then
$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x \implies gh \in \mathrm{Stab}(x)$$

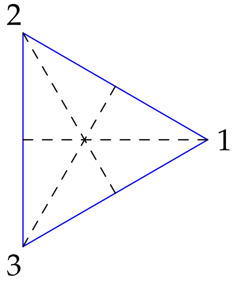
Closure This relies on both parts of the Definition. If $g \in \mathrm{Stab}(x)$, then
$$\begin{aligned} x = g \cdot x &\implies g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x \\ &\implies g^{-1} \in \mathrm{Stab}(x) \end{aligned}$$

■

Example 7.5. The dihedral group $D_3 = \{e, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ acts on the set X of vertices of an equilateral triangle.[27] The fixed sets and stabilizers for this action are as follows:

Element g	$\mathrm{Fix}(g)$
e	$\{1,2,3\}$
ρ_1	$\emptyset$
ρ_2	$\emptyset$
μ_1	$\{1\}$
μ_2	$\{2\}$
μ_3	$\{3\}$

Vertex x	$\mathrm{Stab}(x)$
1	$\{e, \mu_1\}$
2	$\{e, \mu_2\}$
3	$\{e, \mu_3\}$



D_3 also acts on the set of *edges* of the triangle $E = \{\{1,2\},\{1,3\},\{2,3\}\}$. You needn't write all these out since stabilizing an edge is equivalent to stabilizing its opposite vertex. Still, here is the data:

Element g	$\mathrm{Fix}(g)$
e	E
ρ_1	$\emptyset$
ρ_2	$\emptyset$
μ_1	$\{\{2,3\}\}$
μ_2	$\{\{1,3\}\}$
μ_3	$\{\{1,2\}\}$

Edge $\{x,y\}$	$\mathrm{Stab}(\{x,y\})$
$\{1,2\}$	$\{e, \mu_3\}$
$\{1,3\}$	$\{e, \mu_2\}$
$\{2,3\}$	$\{e, \mu_1\}$

Exercises 7.1. Key concepts: *(left) action* $\mathrm{Fix}(g)$ $\mathrm{Stab}(x) \le G$ *faithful & transitive actions*

1. For part 5 of Example 7.2, determine whether each action is faithful and/or transitive.
2. Consider the cyclic subgroup $G = \langle \sigma \rangle$ of S_6 generated by the 6-cycle $\sigma = (1\,2\,3\,4\,5\,6)$.
   (a) State the fixed sets and stabilizers for the natural action of G on the set $X = \{1,2,3,4,5,6\}$.
   (b) Is the action of G faithful? Transitive?
3. Repeat the previous question when $\sigma = (1\,3)(2\,4\,6)$.
4. Mimic Example 7.5 for the actions of D_4 on $X = \{\text{vertices}\}$ and $E = \{\text{edges}\}$ of the square. (*Use whatever notation you like; ρ, μ, δ or cycle notation*)
5. Prove that *left multiplication* of G on itself $g \cdot x = gx$ is:
   (a) *Free*: $\exists x \in G,\ g \cdot x = x \implies g = e$ (this is stronger than faithfulness [$\forall$ versus $\exists$]).
   (b) *Transitive*.
6. Suppose that G acts on itself ($X = G$) by *conjugation* $g \cdot x = gxg^{-1}$.
   (a) Prove that conjugation is faithful if and only if the *center* is trivial: $Z(G) = \{e\}$.
   (b) If G is abelian, is conjugation faithful? Transitive? Explain.
   (c) If $G = S_n$, is conjugation faithful? Transitive? Explain.
7. Suppose G has a left action on X. Prove that G acts faithfully on X if and only if no two distinct elements of G have the same action on every element.

[27] Recall that ρ_1 rotates 120° counter-clockwise, that $\rho_2 = \rho_1^2$ and that μ_i reflects across the altitude through vertex i.

7.2 Orbits & Burnside's Formula

We first met orbits in the context of the symmetric groups S_n. The same idea applies to any action.

Definition 7.6. Let $G \times X \to X$ be an action. The *orbit* of $x \in X$ under G is the set of elements into which x may be transformed:

$$Gx = \{g \cdot x : g \in G\} \subseteq X \qquad \text{(also written } G \cdot x\text{)}$$

Examples 7.7. 1. If $X = \{1, 2, \ldots n\}$ and $G = \langle \sigma \rangle \leq S_n$, then

$$Gx = \{\sigma^k(x) : k \in \mathbb{Z}\} = \mathrm{orb}_x(\sigma)$$

The definition of orbits therefore coincides with that in Section 4.2.

2. A transitive action[28] has only one orbit.

3. If $O_2(\mathbb{R})$ acts on $\mathbb{R}^2$ by matrix multiplication, then the orbits are circles centered at the origin!

Lemma 7.8. *The orbits of an action partition X.*

We omit the proof: compare the special case where S_n acts on $X = \{1, \ldots, n\}$ (Lemma 4.12).
Our next result is analogous to Lemma 6.6 where we counted the number of (left) cosets of $\ker \phi$.

Lemma 7.9. *The cardinality of the orbit Gx is the index of the isotropy subgroup* $\mathrm{Stab}(x)$*:*

$$|Gx| = \big(G : \mathrm{Stab}(x)\big)$$

For a finite group $|G|$, the size of the orbit necessarily divides the order of the group $|G|$.

Proof. Observe that

$$\begin{aligned} g \cdot x = h \cdot x &\iff h^{-1}g \cdot x = x \iff h^{-1}g \in \mathrm{Stab}(x) \\ &\iff g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x) \end{aligned}$$

Otherwise said (contrapositive) distinct elements of Gx correspond to distinct left cosets. ■

Examples 7.10. 1. Let $\sigma = (1\,4)(2\,7\,3) \in S_7$. Consider $X = \{1, 2, 3, 4, 5, 6, 7\}$ under the action of the cyclic group $G = \langle \sigma \rangle$. The orbits are precisely the disjoint cycles: $\{1, 4\}$, $\{2, 3, 7\}$, $\{5\}$, $\{6\}$. Observe that G has six elements:

$$e, \quad \sigma = (1\,4)(2\,7\,3), \quad \sigma^2 = (2\,3\,7), \quad \sigma^3 = (1\,4), \quad \sigma^4 = (2\,7\,3), \quad \sigma^5 = (1\,4)(2\,3\,7)$$

The Lemma is easily verifiable: for instance,

$$\begin{aligned} &\mathrm{Stab}(3) = \{\tau \in G : \tau(3) = 3\} = \{\sigma^k : \sigma^k(3) = 3\} = \{e, \sigma^3\} \\ &\implies \big(G : \mathrm{Stab}(3)\big) = \frac{6}{2} = 3 = |\{2, 3, 7\}| = |G3| \end{aligned}$$

[28] We now have two meanings of *transitive*; one for equivalence relations and one for actions. Be careful!

2. In Exercise 6.3.13 we computed several centralizers (stabilizers under conjugation). Notice what the Lemma says about the size of the orbit of the 3-cycle $\sigma = (1\,2\,3)$ under conjugation:

$$|S_3(\sigma)| = \frac{|S_3|}{|C(\sigma)|} = \frac{3!}{3} = 2$$

As it should be, this is precisely the size of the conjugacy class of 2-cycles!

Burnside's Formula

It can be useful to count the *number* of orbits of an action. For *finite* actions, this can be done in two different ways, which leads to an interesting formula. We start by observing that

$$S = \{(g,x) \in G \times X : g \cdot x = x\} \quad \text{has cardinality} \quad |S| = \sum_{x \in X} |\mathrm{Stab}(x)| = \sum_{g \in G} |\mathrm{Fix}(g)|$$

We now count the elements of S in a different way. Since $(G : \mathrm{Stab}(x)) = \frac{|G|}{|\mathrm{Stab}(x)|}$, we see that

$$\frac{|S|}{|G|} = \sum_{x \in X} \frac{|\mathrm{Stab}(x)|}{|G|} = \sum_{x \in X} \frac{1}{(G : \mathrm{Stab}(x))} = \sum_{x \in X} \frac{1}{|Gx|} \tag{$*$}$$

where we used Lemma 7.9 for the last equality. Consider a fixed orbit Gy. Since $|Gx| = |Gy|$ is *constant* for each $x \in Gy$, we conclude that

$$\sum_{x \in Gy} \frac{1}{|Gx|} = \frac{|Gy|}{|Gy|} = 1$$

The summation $(*)$ therefore counts 1 for *each distinct orbit*. In conclusdion:

Theorem 7.11 (Burnside's formula). *Let G be a finite group acting on a finite set X. Then*

$$\#\,\textit{orbits} = \frac{1}{|G|} \sum_{x \in X} |\mathrm{Stab}(x)| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

Example (7.10.1 cont). Here is the data when $G = \langle \sigma \rangle = \langle (1\,4)(2\,7\,3) \rangle$ acts on $X = \{1,2,3,4,5,6,7\}$:

$x \in X$	$\mathrm{Stab}(x)$
$1,4$	$\{e, \sigma^2, \sigma^4\}$
$2,3,7$	$\{e, \sigma^3\}$
$5,6$	$G = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$

$g \in G$	$\mathrm{Fix}(g)$
e	$X = \{1,2,3,4,5,6,7\}$
σ, σ^5	$\{5,6\}$
σ^2, σ^4	$\{1,4,5,6\}$
σ^3	$\{2,3,5,6,7\}$

Burnside's formula merely sums the cardinalities of all the subsets in the right column of each table:

$$\begin{aligned} 4 = \#\text{ orbits} &= \frac{1}{|G|} \sum_{x \in X} |\mathrm{Stab}(x)| = \frac{1}{6}(3+2+2+3+6+6+2) \\ &= \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| = \frac{1}{6}(7+2+4+5+4+2) \end{aligned}$$

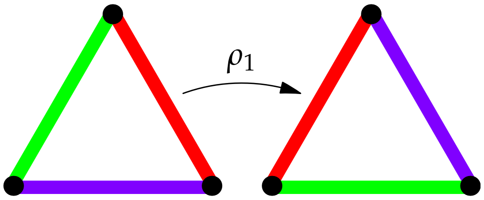
One reason to count the number of orbits of an action is that we often want to consider objects as equivalent if they differ by the action of some group.

Example 7.12. A child's toy consists of a wooden equilateral triangle whose edges are painted using any choice of colors of the rainbow. How many distinct toys could we create?

This might feel like an imprecisely-posed problem, but think for a moment like a child: wouldn't they likely consider the two pictured triangles below to be the same? The language of group actions can help make this precise.

- If we orient each triangle the same way, then a single toy may be considered as an element of $X = \{\text{ordered color triples}\}$. Since there are 7 choices for the color of each edge, we see that $|X| = 7^3 = 343$ (a large set!).

- Two toys are equivalent if they differ only by a rotation in 3-dimensions. This amounts to the natural action of D_3 on X: for instance, taking ρ_1 to rotate 120° counter-clockwise,



$$\rho_1 \cdot (\text{red,green,violet}) = (\text{violet,red,green})$$

The number of distinct toys is therefore the number of orbits of D_3 on X, which we may compute using Burnside. Since it would be time consuming to find the stabilizer of each element of X, we use the fixed set approach.

Identity e: For any action $\text{Fix}(e) = X$.

Rotations ρ_1, ρ_2: If a color-scheme is fixed by ρ_j, then all pairs of adjacent edges must be the same color. Since there are seven colors in the rainbow, we see that $|\text{Fix}(\rho_i)| = 7$.

Reflections μ_1, μ_2, μ_3: Since μ_j swaps two edges, any color-scheme in its fixed set must have these edges the same color. We have 7 choices for the color of the switched edges, and an independent choice of 7 colors for the other edge. It follows that $\left|\text{Fix}(\mu_j)\right| = 7^2 = 49$.

The number of distinct toys is therefore

$$\begin{aligned}\#\,\text{orbits} &= \frac{1}{|D_3|}\sum_{\sigma\in D_3}|\text{Fix}(\sigma)| = \frac{1}{6}(7^3 + \underbrace{7+7}_{\text{rotations}} + \underbrace{7^2+7^2+7^2}_{\text{reflections}})\\ &= \frac{7}{6}(49+1+1+7+7+7) = 84\end{aligned}$$

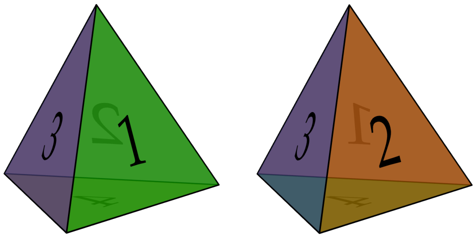
For simpler version of the problem, consider the situation where all sides must be different colors. In this case D_3 acts on a set of color-schemes with cardinality $|Y| = 7\cdot 6\cdot 5 = 210$. Moreover, only the identity element has a non-empty fixed set. The number of distinct three-colored toys is therefore

$$\#\,\text{orbits} = \frac{1}{|D_3|}\sum_{\sigma\in D_3}|\text{Fix}(g)| = \frac{1}{6}(210+0+\cdots+0) = \frac{210}{6} = 35$$

Of course you are welcome to answer questions like these using pure combinatorics without any resort to group theory!

Example 7.13 (Dice-rolling for Geeks). Various games (such as Dungeons & Dragons) make use of polyhedral dice beyond merely the cube (see, for instance, Exercise 2.4.12).

Since dice are for rolling, we consider two such to be equivalent if one can be rotated into the other. It shouldn't be hard to convince yourself that the pictured tetrahedral dice are distinct (non-equivalent): the first *cannot* be rotated to make the second.



Indeed, it is not difficult to see that these are the *only* tetrahedral dice: if you place 4 on the table, then the remaining faces must be numbered 1, 2, 3 either *counter-clockwise* or *clockwise*.

For larger dice, such a counting approach is impractical. However, with a little thinking about symmetry groups, Burnside's formula will ride to the rescue.

Suppose a regular polyhedron has f faces, each with n sides.

- The faces may be labelled 1 thorough f in $f!$ distinct ways. Denote the set of distinct labellings by X.
- We may rotate the polyhedron so that any face is mapped to any other, *in any orientation.* For instance, the face labelled 1 may be rotated to any of the f faces, before rotating the polyhedron around that face in any of n orientations. The rotation group G of the polyhedron therefore has fn elements.
- Each non-identity element of the rotation group G moves at least one face, whence

$$|\mathrm{Fix}(g)| = \begin{cases} X & \text{if } g = e \\ \emptyset & \text{if } g \neq e \end{cases}$$

- By Burnside's formula, the number of distinct dice for a regular polyhedron is therefore

$$\#\text{ orbits} = \frac{1}{|G|}\,|\mathrm{Fix}(e)| = \frac{|X|}{|G|} = \frac{f!}{fn} = \frac{(f-1)!}{n}$$

Here is the complete data for all the regular platonic solids.

Polyhedron	f	n	Rotation Group	# distinct dice (orbits)
Tetrahedron	4	3	A_4	2
Cube	6	4	S_4	30
Octahedron	8	3	S_4	1,680
Dodecahedron	12	5	A_5	7,983,360
Icosahedron	20	3	A_5	40,548,366,802,944,000

Note that we don't need an explicit description of the rotation group, only its *order* $|G|$. We saw that the rotation group of regular tetrahedron was A_4 in Example 4.26.3. Proving that the remaining groups are as claimed is somewhat trickier...

Exercises 7.2. Key concepts: *Orbits partition X* $|Gx| = (G : \text{Stab}(x))$ *Burnside's formula*

1. Determine the orbits of $G = \langle \sigma \rangle$ on $X = \{1, 2, 3, 4, 5, 6\}$ for each of Exercises 7.1.2 and 3. In both cases verify Burnside's formula.

2. Revisit Example 7.12. How may distinct toys may be created if:

   (a) A maximum of two colors can be used?

   (b) Exactly two colors must be used?

3. Prove Lemma 7.8: the orbits of a (left) action partition X.

4. Revisit Exercise 6.3.13 and Example 7.10.2. Prove that there are two distinct conjugacy classes of 5-cycles in A_5. Provide an example of two 5-cycles which are not conjugate in A_5.

5. A 10-sided die (see Exercise 2.4.12) is shaped so that all faces are congruent *kites*: five faces are arranged around the north pole and five around the south.

   (a) Argue that the group of rotational symmetries of such a die has ten elements, and that it is isomorphic to D_5.

   (b) Use Burnside's formula to determine how many distinct 10-sided dice (faces numbered 1 to 10) may be produced.

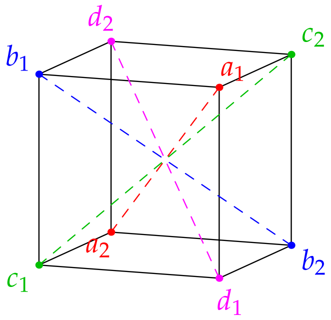
6. A soccer ball is constructed from 20 regular hexagons and 12 regular pentagons as in the picture.
   Suppose the 20 hexagonal patches are all to have different colors, as are the 12 pentagonal patches. How many distinct balls may be produced?

7. The faces of a cuboid measuring $1 \times 1 \times 2$ in are to be painted using (at most) two colors. Up to equivalence by rotations, how many ways can this be done?

8. Repeat the previous question for a regular tetrahedron.

9. (Hard) A cube has four *diagonals*: a, b, c, d, which are permuted by its rotation group. For instance, we might rotate by 180° around an axis through the midpoints of the sides $\overline{a_1 b_1}$ and $\overline{a_2 b_2}$. This switches diagonals a and b, but leaves c and d alone and therefore acts as the 2-cycle $(a\,b)$ on $\{a, b, c, d\}$. As a function on vertices,

$$(a\,b) : \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \end{pmatrix} \mapsto \begin{pmatrix} b_1 & a_1 & c_2 & d_2 \\ b_2 & a_2 & c_1 & d_1 \end{pmatrix}$$



   (a) Describe as best you can how to rotate the cube in a way that corresponds to each of the following rotations (written in cycle notation):

   $$(a\,b\,c), \quad (a\,b\,c\,d), \quad (a\,b)(c\,d)$$

   Hence argue that the rotation group of the cube is isomorphic to S_4.

   (b) A cube can operate as a "3-sided" die by labelling two each of its faces using the numbers 1, 2, 3. In how many distinct ways can this be done?

7.3 The Class Equation, *p*-groups, and the Theorems of Cauchy and Sylow

The toolkit provided by group actions is central to an enormous topic: the classification of groups and their internal structure. This final section offers a small taste of this discussion.

Suppose G acts on a finite set X. Denote the set of 1-element orbits by

$$X_G = \bigcap_{g\in G} \mathrm{Fix}(g) = \{x \in X : \forall g \in G, g\cdot x = x\}$$

Let $x_1,\ldots,x_r$ be representatives of the remaining (larger) orbits. Since the orbits partition X,

$$|X| = |X_G| + \sum_{j=1}^{r} |Gx_j| = |X_G| + \sum_{j=1}^{r} (G:\mathrm{Stab}(x_j)) = |X_G| + \sum_{j=1}^{r} \frac{|G|}{|\mathrm{Stab}(x_j)|} \qquad (*)$$

We focus on the special case when G acts on itself ($X = G$) by *conjugation* $g\cdot x = gxg^{-1}$.

- The 1-element orbits comprise the group *center*: $X_G = Z(G)$.
- In this context the stabilizer of an element $x \in G$ is known as its *centralizer*:

  $$C(x) = \mathrm{Stab}(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$$

- Equation $(*)$ is called the *class equation*:

$$\boxed{|G| = |Z(G)| + \sum_{j=1}^{r} |\text{conjugacy class of } x_j| = |Z(G)| + \sum_{j=1}^{r} \frac{|G|}{|C(x_j)|}}$$

Example 7.14. The conjugacy classes in S_4 are the cycle-types, so the class equation is easily verified:

$$24 = |\{e\}| + \#(\text{2-cycles}) + \#(\text{3-cycles}) + \#(\text{4-cycles}) + \#(\text{2,2-cycles}) = 1+6+8+6+3$$

Our next result applies the class equation to obtain a partial converse to Lagrange's Theorem.

Theorem 7.15 (Cauchy). *If a prime p divides $|G|$, then G contains a subgroup/element of order p.*

Proof.

1. Exercise 9 supplies an inductive proof that abelian G have such subgroups.
2. If G is non-abelian, then the center $Z(G)$ is a proper (abelian) subgroup.

   Let $x \notin Z(G)$. Plainly $C(x)$ is a proper subgroup of G. If p does not divide $|C(x)|$, then p divides $|Gx| = (G : C(x)) = \frac{|G|}{|C(x)|}$. If this holds for all non-trivial orbits, the class equation says that $|Z(G)|$ is divisible by p. Either way, G has a **proper subgroup** H whose order is divisible by p.

   If H is abelian, apply case 1. Otherwise, repeat starting with H to find an even smaller subgroup whose order is divisible by p. If this process never reached an abelian subgroup, then we'd have an infinite descending sequence of proper subgroups: contradiction.

The resulting subgroup is cyclic (Corollary 5.10), whence an element of order p also exists. ■

Example 7.16. If G has order $60 = 2^2 \cdot 3 \cdot 5$, then it has subgroups of orders 2, 3 and 5. It also has subgroups of other orders (at the very least 1, 60 and 4 — this last by the 1st Sylow Theorem below).

Haven't we done this already? Exercise 3.3.14 appears to cover abelian groups, but this depends on the Fundamental Theorem (3.26), the standard proof of which in fact relies on Cauchy (Exercise 10)!

Definition 7.17. Let p be a prime. A group G is a *p-group* if all its elements have order a power of p.

Examples 7.18. 1. $G = \mathbb{Z}_8$ is a 2-group.

2. $G = \langle 2 \rangle$ $(\cong \mathbb{Z}_9)$ is a 3-subgroup of $\mathbb{Z}_{18}$ (this last is not a 3-group).
3. $\mathbb{Z}_3 \times \langle 2 \rangle$ is a 3-subgroup of $\mathbb{Z}_3 \times \mathbb{Z}_6$.
4. $V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a 2-subgroup of S_4.

The proofs of the next result are exercises.

Theorem 7.19. 1. *A finite group G is a p-group if and only if $|G| = p^n$ for some n.*

2. *If G is a p-group, then its center $Z(G)$ is non-trivial.*

Corollary 7.20. *Let p be prime. If G has order p^2, then it is abelian.*

Proof. By the Theorem, we know that $|Z(G)| = p$ or p^2. In the second case we are done: $Z(G) = G$ says that G is abelian. In the first case the factor group is cyclic:

$$\left| {}^{G}\!/_{Z(G)} \right| = p \implies {}^{G}\!/_{Z(G)} \cong \mathbb{Z}_p$$

Exercise 6.3.14 says G is abelian, though really it's a contradiction: $Z(G) = G \implies {}^{G}\!/_{Z(G)} \cong \mathbb{Z}_1$. ∎

Our final results go some way towards establishing the existence and number of certain subgroups. We omit the proofs: a typical approach uses induction with Cauchy's Theorem as the base case, and the application of various ingenious group actions. If you are interested, look them up!

Theorem 7.21 (Sylow). *Let G be finite and write $|G| = p^n m$, where p is prime and $\gcd(p, m) = 1$.*

1. *G contains a subgroup H_{p^i} of order p^i for each $i = 1, \ldots, n$. Moreover, any such subgroup with $i < n$ is a normal subgroup of some subgroup of order p^{i+1}:*

$$\{e\} \lhd H_p \lhd H_{p^2} \lhd \cdots \lhd H_{p^n} \le G \tag{†}$$

2. *Any two maximal p-subgroups H_{p^n} (called* Sylow p-subgroups*) are conjugate.*
3. *The number of Sylow p-subgroups divides $|G|$ and is congruent to 1 modulo p.*

Only the last inclusion in (†) can be non-normal. For a given example, the 3rd Theorem might show that there is a *unique* Sylow p-subgroup H_{p^n}: by Exercise 6.3.5, such a subgroup is necessarily normal.

Examples 7.22. 1. Suppose $|G| = 15 = 3 \cdot 5$. By the 1st Sylow Theorem, G has at least one Sylow 3-subgroup (isomorphic to $\mathbb{Z}_3$) and at least one Sylow 5-subgroup (isomorphic to $\mathbb{Z}_5$).

The divisors of 15 are listed, along with whether each is congruent to 1 modulo 3 or 5. By the 2nd and 3rd Theorems, G has exactly one subgroup isomorphic to $\mathbb{Z}_3$ and one to $\mathbb{Z}_5$: being self-conjugate, both subgroups are normal.

Divisor d	1	3	5	15
$d \equiv 1 \pmod 2$?	✓			
$d \equiv 1 \pmod 3$?	✓			

By Lagrange, the orders of elements in G can only be 1, 3, 5 or 15. Since an order 3 element generates a subgroup isomorphic to $\mathbb{Z}_3$ (the *unique* Sylow 3-subgroup), only two elements in G have order 3. Similarly only four elements in G have order 5 (each being a generator of the unique Sylow 5-subgroup). Since only the identity has order 1, the remaining $8 = 15 - 1 - 2 - 4$ elements must have order 15, and thus generate G.

In conclusion: if $|G| = 15$, then $G \cong \mathbb{Z}_{15}$ is cyclic. Exercise 5 extends this analysis to when $|G| = pq$, where $p < q$ are primes for which $q - 1$ is not divisible by p: in such a case $G \cong \mathbb{Z}_{pq}$.

2. Suppose $|G| = 100 = 2^2 \cdot 5^2$. By the 1st Sylow Theorem, G has at least one Sylow 5-subgroup of order $5^2 = 25$, and at least one Sylow 2-subgroup of order $4 = 2^2$. We can be more precise by applying the other results.

The full list of divisors of $|G| = 100$ is: 1, 2, 4, 5, 10, 20, 25, 50, 100.

- The only divisor congruent to 1 modulo 5 is 1 itself! By the 3rd Theorem, there is precisely one Sylow 5-subgroup H_{25} of G. Since this is the only subgroup of order 25, it must be normal: $H_{25} \lhd G$. By Corollary 7.20, H_{25} is abelian. The Fundamental Theorem says that either $H_{25} \cong \mathbb{Z}_{25}$ or $H_{25} \cong \mathbb{Z}_5 \times \mathbb{Z}_5$.
- The divisors 1, 5 and 25 are congruent to 1 modulo 2, so there might be 1, 5 or 25 distinct Sylow 2-subgroups of G.

We give several sub-examples where the Sylow p-subgroups can be seen explicitly.

(a) $G = \mathbb{Z}_{100}$ has one Sylow 5-subgroup $\langle 4 \rangle \cong \mathbb{Z}_{25}$, and one Sylow 2-subgroup $\langle 25 \rangle \cong \mathbb{Z}_4$.

(b) $G = \mathbb{Z}_{50} \times \mathbb{Z}_2$ has one Sylow 5-subgroup $\langle (2, 0) \rangle \cong \mathbb{Z}_{25}$, and one Sylow 2-subgroup $\langle 25 \rangle \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) $G = \mathbb{Z}_5 \times \mathbb{Z}_{20}$ has one Sylow 5-subgroup $\mathbb{Z}_5 \times \langle 4 \rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_5$, and one Sylow 2-subgroup $\langle (0, 5) \rangle \cong \mathbb{Z}_4$.

(d) $G = D_{50}$ has one Sylow 5-subgroup consisting of half the 50 rotations:

$$\langle \rho_2 \rangle = \{\rho_0, \rho_2, \ldots, \rho_{48}\} \cong \mathbb{Z}_{25}$$

There are 25 distinct Sylow 2-subgroups, each of which is isomorphic to the Klein 4-group V. These may be described explicitly if we label the reflections $\mu_1, \ldots, \mu_{50}$:

$$V_i = \{\rho_0, \rho_{25}, \mu_i, \mu_{i+25}\}, \quad i = 1, \ldots, 25$$

Note that D_{50} has no subgroups isomorphic to $\mathbb{Z}_4$ (reflections have order 2 and rotations have orders 1, 5 or 25). This is also clear from the 2nd Theorem: all Sylow 2-subgroups are conjugate and thus isomorphic (to V).

Exercises 7.3. 1. State all the 3-subgroups of $\mathbb{Z}_{36}$.

2. Let p be a prime of your choice. In contrast to Corollary 7.20, give an example of a non-abelian group of order p^3.

3. Suppose $|G| = 225 = 3^2 \cdot 5^2$. Prove that G has a normal subgroup of order 25.

4. Suppose $|G| = 20 = 2^2 \cdot 5$.

   (a) Determine how many distinct Sylow 2- and Sylow 5-subgroups G can have. Must they be normal subgroups?

   (b) Similarly to Example 7.22.2, state the Sylow subgroups when

      i. $G = \mathbb{Z}_{20}$, ii. $G = D_{10}$

5. Let G have order pq, where $p < q$ are distinct primes (≥ 3). Then all proper subgroups of G are cyclic (isomorphic to $\mathbb{Z}_p$, $\mathbb{Z}_q$ or $\mathbb{Z}_1$).

   (a) If $pq = 2 \cdot 3 = 6$, then $G \cong \mathbb{Z}_6$ or $\cong S_3$. State all the Sylow 2- and 3-subgroups in each case.

   (b) Returning to the general case, prove that there is a unique Sylow q-subgroup $H \cong \mathbb{Z}_q$ (which is therefore normal) by showing that $p \equiv 1 \pmod{q}$ is a contradiction.

   (c) Suppose moreover that $q - 1$ is not divisible by p. Prove that there is a unique Sylow p-subgroup $K \cong \mathbb{Z}_p$ (which is also normal). Extending the analysis of Example 7.22.1, prove that $G \cong \mathbb{Z}_{pq}$.

   (d) If $|G| = 21$ ($p = 3, q = 7$), show that there are either one or seven Sylow 3-subgroups. In the former case, argue that $G \cong \mathbb{Z}_{21}$.

   (The latter case [seven 3-subgroups] results in a new non-abelian group not seen in these notes.)

6. Prove Theorem 7.19, part 1.

   (*Hints: one direction uses Lagrange's Theorem, the other Cauchy*)

7. Suppose G is a p-group which acts on a finite set X.

   (a) Prove that $|X| \equiv |X_G| \pmod{p}$.

   (*Hint: what can you say about $|Gx|$ if x lies in a non-trivial orbit?*)

   (b) Prove part 2 or Theorem 7.19, that p divides the order of the center $Z(G)$.

8. The alternating group A_5 has order $60 = 2^2 \cdot 3 \cdot 5$ and comprises the identity, all 3-cycles, 5-cycles, and 2,2-cycles in S_5.

   (a) Describe all the Sylow 2-, 3-, and 5-subgroups of A_5 and verify that the number of each is in line with the 3rd Theorem.

   (b) Extending Exercise 7.2.4, find the sizes of all conjugacy classes in A_5. Hence prove that A_5 is a *simple group*: if N is a normal subgroup of A_5, then $N = \{e\}$ or A_5.

   (Simple groups are very important and have applications throughout mathematics. Their full classification was completed in 2004—an enormous undertaking: look it up...)

9. We prove the abelian part of Cauchy's Theorem by induction on the order of G.

   (a) Explain why the base case $|G| = 2$ is true.

   Fix $n \geq 3$, let G be abelian of order n and assume p divides n. For the induction hypothesis, assume that if K is *any* abelian group of order $|K| < n$ where p divides $|K|$, then K has a subgroup of order p.

   - Let $x \in G$ be a non-identity element with order $m = |\langle x \rangle|$ (necessarily $m \geq 2$).
   - Choose a prime q dividing m, define $y := x^{m/q}$ and let $H := \langle y \rangle$.

   (b) What is the order of H? Explain why are we done if $q = p$.

   (c) If $q \neq p$, use the induction hypothesis to explain why there exists a coset $zH \in {}^{G}/_{H}$ of order p. Now prove that z^q has order p in G.

10. We sketch part of the proof of the Fundamental Theorem of Finite Abelian Groups (3.26).

    Suppose G is abelian and that $|G| = p^n m$ where p does not divide m. Define

$$H = \{x \in G : x^{p^n} = e\}, \qquad K = \{x \in G : x^m = e\}$$

   (a) Show that H is a p-group.

   (b) Since $\gcd(m, p^n) = 1$, we may write $1 = \kappa m + \lambda p^n$ for some $\kappa, \lambda \in \mathbb{Z}$.

      i. For any $x \in G$, prove that $x^{\kappa m} \in H$ and $x^{\lambda p^n} \in K$.

      ii. Prove that the following function is an isomorphism:

$$\psi : G \to H \times K : x \mapsto \left(x^{\kappa m}, x^{\lambda p^n}\right)$$

      (*Hint: try evaluating* $\psi(hk)\ldots$).

   (c) Prove that $|H| = p^n$ by applying Cauchy's Theorem to show that p does not divide $|K|$.

   (Inducting on this shows that $G \cong H_1 \times \cdots \times H_k$ where each H_j is a p_j-group of maximal order. A little more work is needed to show that each H_j is itself a direct product of cyclic groups and thus complete the proof.)