# UNSW Mathematics Society Presents
# MATH3711/5706 Seminar

**Presented by James Davidson, Bruce Chen, and Gerald Huang**

# Overview I

1. Introduction to Group Theory
2. Group Homomorphisms
3. Direct Products and Sums
4. Group Actions
5. Rings
   Domains and Fraction Fields
   Unique Factorisation Domains and Euclidean Domains
   Gauss' Lemma
6. Fields and Their Extensions
   Finite fields

# 1. Introduction to Group Theory

# Groups

## Definition (Group)

A *group* is a set $G$ equipped with a *multiplication map* $* : G \times G \to G$ satisfying the group axioms:

(G1) The multiplication $*$ is *associative*: that is, for all $g, h, k \in G$ we have $g * (h * k) = (g * h) * k$.

(G2) There exists an *identity element* $1_G \in G$ such that $g * 1_G = 1_G * g = g$ for all $g \in G$.

(G3) For each $g \in G$, there exists an *inverse element* $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = 1$.

# Group notation

If the multiplication map is well-understood, it is common to refer to the set $G$ interchangeably with the group proper $(G, *)$, and write $gh$ instead of $g * h$. The identity can also just be written as 1, omitting the explicit mention of $G$. Moreover, for $n \in \mathbb{Z}$, we write

$$g^n = \begin{cases} gg \cdots g & \text{if } n > 0 \\ 1 & \text{if } n = 0 \\ g^{-1}g^{-1} \cdots g^{-1} & \text{if } n < 0 \end{cases}$$

where each multiplication involves $n$ terms.

# Useful facts about groups

**Theorem**

Let $G$ be a group. It follows from axioms (G1) – (G3) that

(1) The identity element of $G$ is unique.

(2) The inverse element $g^{-1}$ for each $g \in G$ is unique.

(3) For any $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.

(4) For any $g \in G$ and $m, n \in \mathbb{Z}$, $g^{m+n} = g^m g^n$ and $(g^m)^n = g^{mn}$. In particular, this implies $(g^{-1})^{-1} = g$ and $(g^n)^{-1} = g^{-n}$.

In other words, groups follow many natural properties. The first two statements justify the notation used for identity and inverse elements.

# Order of elements and groups

## Definition (Order of an element)

For each $g \in G$, the *order of* $g$ is the least positive integer $n$ such that $g^n = 1$. In this case, we write $\text{ord}(g) = n$. If no such integer exists, the element is said to have *infinite order*.

## Definition (Order of a group)

The *order of a group* $G$ the cardinality of $G$, i.e. $|G|$. If $|G| < \infty$, the group is said to be *finite*.

# Subgroups

**Definition (Subgroup)**

Let $(G, *)$ be a group, and suppose that $\emptyset \neq H \subseteq G$. If $(H, *)$ is a group, then $H$ is said to be a *subgroup* of $G$, and we write $H \leq G$.

**Theorem (Subgroup test)**

Let $G$ be a group. Any $\emptyset \neq H \subseteq G$ is a subgroup of $G$ if and only if

(SG1) For every $h, k \in H$, we have $hk \in H$.

(SG2) For each $h \in H$, $h^{-1} \in H$.

Proving that a set is a subgroup of another group via this test is a useful way to prove that it forms a group in the first place.

# A proof involving subgroups

**Original example**

Let $G$ be a group with an element $g$ such that $H = G - \{g\}$ is a subgroup of $G$. Show that $|G| = 2$.

*Proof.* Take $h \in H$.

# A proof involving subgroups

**Original example**

Let $G$ be a group with an element $g$ such that $H = G - \{g\}$ is a subgroup of $G$. Show that $|G| = 2$.

*Proof.* Take $h \in H$. We cannot have $gh^{-1} \in H$, as otherwise

# A proof involving subgroups

**Original example**

Let $G$ be a group with an element $g$ such that $H = G - \{g\}$ is a subgroup of $G$. Show that $|G| = 2$.

*Proof.* Take $h \in H$. We cannot have $gh^{-1} \in H$, as otherwise (SG1) implies that $(gh^{-1})h = g \in H$.

# A proof involving subgroups

**Original example**

Let $G$ be a group with an element $g$ such that $H = G - \{g\}$ is a subgroup of $G$. Show that $|G| = 2$.

*Proof.* Take $h \in H$. We cannot have $gh^{-1} \in H$, as otherwise (SG1) implies that $(gh^{-1})h = g \in H$. But $g$ is the only element not in $H$, so $gh^{-1} = g$, i.e. $h = 1$. Thus $|H| = 1$ and $|G| = 2$. □

# An important group: $S_n$

**Example (Symmetric group)**

With $S = \{1, 2, \ldots, n\}$, define $S_n := \text{Perm}(S)$ to be the set of permutations $\sigma : S \to S$ (i.e. bijections). This set forms a group once equipped with $\circ$ as a multiplication: the *symmetric group on $n$ letters*.

An immediate consequence of this definition is that $|S_n| = n!$.

# Element representations in $S_n$

## Definition (Two-line and cycle notations)

Any element $\sigma \in S_n$ can be described in *two-line notation* as

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

or in *cycle notation* as $(i_1\ i_2\ \dots\ i_k)$, where

$$\begin{cases} \sigma(i_j) = i_{j+1} & \text{for } 1 \leq j < k \\ \sigma(i_k) = i_1 & \\ \sigma(i) = i & \text{for } i \notin \{i_1, i_2, \dots, i_k\} \end{cases}.$$

The permutation in this latter notation is called a *k-cycle*, since such a cycle has order $k$ in $S_n$.

# Cycles

## Definition (Transposition)

A *transposition* is a cycle of order 2. A transposition is *basic* if it is of the form $(i\ i+1)$.

## Definition (Disjoint cycles)

Two cycles $(i_1\ i_2\ \ldots\ i_k)$ and $(j_1\ j_2\ \ldots\ j_\ell)$ are said to be *disjoint* if

$$\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_\ell\} = \emptyset.$$

# Useful facts about cycles

**Theorem**

(1) If $\sigma$ and $\tau$ are disjoint cycles, then they commute, i.e. $\sigma\tau = \tau\sigma$.

(2) We have $(i_1\ i_2\ \ldots\ i_k) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{k-1}\ i_k)$.

(3) More generally, any permutation $\sigma \in S_n$ can be expressed as a product of disjoint cycles, as a product of transpositions or as a product of basic transpositions.

# The sign of a permutation

**Definition (Sign of a permutation)**

The *sign* of a permutation $\sigma \in S_n$, denoted $s(\sigma)$, is an indication of how many *inversions* it creates, i.e. pairs $(x, y)$ with $x < y$ and $\sigma(x) > \sigma(y)$. If there are an even number of inversions, then $s(\sigma)$ is 1 and $\sigma$ is said to be an *even permutation*. Otherwise, $s(\sigma) = -1$, and $\sigma$ is said to be an *odd permutation*.

# Useful facts about signs

**Theorem**

(1) If $\sigma, \tau \in S_n$, then $s(\sigma\tau) = s(\sigma)s(\tau)$.

(2) The sign of any transposition is $-1$.

(3) If $\sigma = \tau_1\tau_2\cdots\tau_k$ for transpositions $\tau_i$, then $s(\sigma) = (-1)^k$.

The last statement gives a much more workable alternative definition for calculating signs in practice, and is often the one to use (provided that the decomposition into transpositions is not too involved).

# A sign-based subgroup: $A_n$

**Definition (Alternating group)**

Consider the subset $A_n$ of $S_n$ consisting of even permutations, that is,

$$A_n = \{\sigma \in S_n : s(\sigma) = 1\}.$$

This forms a subgroup of $S_n$: the *alternating group*.

# Generators

The fact that the intersection of arbitrarily many subgroups remains a subgroup motivates the definition of a particular type of subgroup.

**Definition (Subgroup generated by a set)**

Let $G$ be a group, and let $\emptyset \neq S \subseteq G$. If $\mathcal{H}$ is the collection of all subgroups $H \leq G$ with $S \subseteq H$, the subgroup

$$\langle S \rangle = \bigcap_{H \in \mathcal{H}} H$$

is called the *subgroup generated by* $S$.

One consequence is that $\langle S \rangle$ is the *smallest* subgroup with $S \subseteq \langle S \rangle$.

# Generators (continued)

An alternative characterisation of generated subgroups in terms of their element structure is the following.

**Theorem**

Let $G$ be a group, and $S \subseteq G$. Then

$$\langle S \rangle = \{s_1 s_2 \cdots s_n : s_i \in S \cup S^{-1} \text{ for some } n \geq 0\},$$

where $S^{-1} = \{s^{-1} : s \in S\}$. When $n = 0$, notionally $s_1 s_2 \cdots s_n = 1$.

# Finitely-generated groups

**Definition (Finitely-generated group)**

A group $G$ is said to be *finitely generated* if there exists some finite subset $S = \{s_1, s_2, \ldots, s_n\}$ with $G = \langle S \rangle = \langle s_1, s_2, \ldots, s_n \rangle$. The set $S$ is then called a *generating set of* $G$. If $G = \langle g \rangle$ for some $g \in G$, then the group $G$ is said to be *cyclic*, with $g$ one of its *generators*.

Do note however that finitely-generated groups are not necessarily finite groups: consider $\mathbb{Z} = \langle 1 \rangle$, for example.

# A proof involving cyclic groups

**Original example**

Prove that $(\mathbb{Q}, +)$ is not cyclic.

*Proof.* If it was the case that

$$\mathbb{Q} \stackrel{!}{=} \left\langle \frac{a}{b} \right\rangle$$

# A proof involving cyclic groups

**Original example**

Prove that $(\mathbb{Q}, +)$ is not cyclic.

*Proof.* If it was the case that

$$\mathbb{Q} \stackrel{!}{=} \left\langle \frac{a}{b} \right\rangle = \left\{ \frac{na}{b} : n \in \mathbb{Z} \right\},$$

then it would follow that

# A proof involving cyclic groups

**Original example**

Prove that $(\mathbb{Q}, +)$ is not cyclic.

*Proof.* If it was the case that

$$\mathbb{Q} \stackrel{!}{=} \left\langle \frac{a}{b} \right\rangle = \left\{ \frac{na}{b} : n \in \mathbb{Z} \right\},$$

then it would follow that $a/2b$ is an *integer* multiple of $a/b$, which is obviously false. So $\mathbb{Q}$ cannot be generated by a single element. □

# An important finitely-generated group: $D_n$

**Example (Dihedral group)**

For $n \geq 3$, a regular $n$-gon has two basic symmetries: a rotation $\sigma$ about its centre by $\frac{2\pi}{n}$, and a reflection $\tau$ in a line through the midpoint of one side and the opposite vertex. Moreover, $\sigma$ and $\tau$ satisfy the skew-commutativity relation $\tau\sigma = \sigma^{-1}\tau$. The group

$$D_n = \langle \sigma, \tau \rangle = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{k-1}\tau\}$$

under $\circ$ of all symmetries of the $n$-gon is called the *dihedral group*.

In particular, $|D_n| = 2n$, $\text{ord}(\sigma) = n$ and $\text{ord}(\tau) = 2$. More generally, elements of the form $\sigma^k\tau$ are reflections, so $\text{ord}(\sigma^k\tau) = 2$.

# Subgroup structure of $D_n$

**Theorem (Subgroups of $D_n$)**

Any subgroup of $D_n$ is one of two alternatives:

(1) A cyclic subgroup of rotational symmetries $\langle \sigma^k \rangle$, where $k \mid n$.

(2) A subgroup of rotational and reflective symmetries of the form $\langle \sigma^k, \sigma^\ell \tau \rangle$ where $k \mid n$.

The second kind of subgroup resembles a "smaller" dihedral group.

# Dihedral group example

## 2009 exam, Q2(c)

Let $D_n$ be the dihedral group generated by the matrices

$$\sigma = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Such a group is *crystallographic* if $4\cos^2\frac{\pi}{n}$ is an integer.

(i) Find all $n$ for which $D_n$ is crystallographic.

(ii) Identify the geometric figure associated with each of the crystallographic dihedral groups.

# Dihedral group example (continued)

*Solution, (i).* Let $x = 4\cos^2 \frac{\pi}{n}$. Since $0 \leq x \leq 4$, it suffices to consider the cases where $x \in \{0, 1, 2, 3, 4\}$, and in those cases just the solutions for positive integers $n$:

- If $x = 0$, then $\cos \frac{\pi}{n} = 0$, which has solution $n = 2$.
- If $x = 1$, then $\cos \frac{\pi}{n} = \pm\frac{1}{2}$, which has solution $n = 3$.
- If $x = 2$, then $\cos \frac{\pi}{n} = \pm\frac{1}{\sqrt{2}}$, which has solution $n = 4$.
- If $x = 3$, then $\cos \frac{\pi}{n} = \pm\frac{\sqrt{3}}{2}$, which has solution $n = 6$.
- If $x = 4$, then $\cos \frac{\pi}{n} = \pm 1$, which has solution $n = 1$.

(The restriction to positive $n$ implies further that $0 \leq \cos \frac{\pi}{n} \leq 1$, so in fact the above solutions come from taking the positive square root.)

# Dihedral group example (continued)

*Solution, (ii).* The obvious geometric associations are that

- $D_3$ is the symmetry group of an equilateral triangle.
- $D_4$ is the symmetry group of a square.
- $D_6$ is the symmetry group of a regular hexagon.

# Dihedral group example (continued)

*Solution, (ii).* The obvious geometric associations are that

- $D_3$ is the symmetry group of an equilateral triangle.
- $D_4$ is the symmetry group of a square.
- $D_6$ is the symmetry group of a regular hexagon.

For $D_1$, we can imagine that it is the symmetry group of a single point with a self-loop,

# Dihedral group example (continued)

*Solution, (ii).* The obvious geometric associations are that

- $D_3$ is the symmetry group of an equilateral triangle.
- $D_4$ is the symmetry group of a square.
- $D_6$ is the symmetry group of a regular hexagon.

For $D_1$, we can imagine that it is the symmetry group of a single point with a self-loop, and for $D_2$, we can imagine that it is the symmetry group of a pair of points, with 2 different edges between them.

The dihedral groups $D_1, D_2$ are too small to be symmetry groups of an $n$-gon in the usual sense. $D_1$ is the group $\{1, r\}$ of two elements. So it is a cyclic group, as is $C_2$. But the nontrivial element of $D_1$ is a reflection, while in $C_2$ it is rotation through the angle $\pi$. The group $D_2$ contains the four elements $\{1, \rho, r, \rho r\}$ , where $\rho = \rho_\pi$. It is isomorphic to the Klein four group. If we like, we can think of $D_1$ and $D_2$ as groups of symmetry of the 1-gon and 2-gon:

1-gon. 2-gon.

Figure: an excerpt from *Algebra* (Michael Artin)

# Cosets

## Definition (Left coset)

Let $G$ be a group, and $H \leq G$ a subgroup. A *left coset of $H$ in $G$* is a set of the form

$$gH = \{gh : h \in H\}$$

for some $g \in G$. The set of left cosets of $H$ in $G$ is

$$G/H = \{gH : g \in G\}.$$

We may define right cosets $Hg$ in a similar way: the set of all such cosets is (perhaps confusingly) written $H \setminus G$. There are analogues for the major results concerning left cosets, so it suffices to simply work with left cosets instead. This is **not** to say, however, that left cosets and right cosets are the same!

# An important example of cosets in $\mathbb{Z}$

## Example (Cosets in $\mathbb{Z}$)

Consider the additive group $(\mathbb{Z}, +)$, and let $m\mathbb{Z} = \{mn : n \in \mathbb{N}\} \leq \mathbb{Z}$. The associated cosets are of the form

$$\overline{r} = r + m\mathbb{Z} = \{r + mq : q \in \mathbb{Z}\}$$

for all integers $0 \leq r < m$, each corresponding to the set of integers whose remainder is $r$ upon division by $m$. Put another way,

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\},$$

and every integer $n \in \mathbb{Z}$ appears in exactly one of these cosets. This is not just some coincidence!

# Cosets as equivalence classes

**Theorem (Equivalence relation characterisation of cosets)**

Let $\sim$ be the equivalence relation on a group $G$ defined by

$$g \sim g' \quad \text{if and only if} \quad g' \in gH$$

for a fixed subgroup $H \leq G$. Then each left coset $gH$ is an equivalence class of $\sim$. Moreover, there is a *disjoint* union

$$G = \dot{\bigcup_{g \in \mathcal{R}}} gH$$

for a suitable set of representatives $\mathcal{R}$ from each equivalence class.

# Index of a subgroup

**Definition (Index of a subgroup)**

The *index of a subgroup* $H \leq G$ is the number of left cosets of $H$ in $G$, and is denoted $[G : H]$. Equivalently, $[G : H] = |G/H|$.

# Lagrange's theorem

The relationship between a subgroup's order and its index is captured by Lagrange's theorem.

**Theorem (Lagrange's theorem)**

Let $G$ be a *finite* group. Then for each subgroup $H \leq G$, $|H|$ divides $|G|$, and $[G : H] = |G/H| = |G|/|H|$.

# Normal subgroups

**Definition (Normal subgroup)**

Let $G$ be a group. If $N \leq G$ is a subgroup with $gN = Ng$ for each $g \in G$, then $N$ is called a *normal subgroup* of $G$, and we write $N \trianglelefteq G$.

**Theorem (Alternative definition of a normal subgroup)**

A subgroup $N \leq G$ is normal if and only if for each $g \in G$ and $n \in N$, we have that $gng^{-1} \in H$.

Despite the name, most subgroups are not normal! In practice, this subset check is the least involved way of checking normality.

# Quotient groups, definitionally

## Definition (Subset multiplication)

Given two nonempty subsets $J, K$ of a group $G$, we define

$$JK = \{jk : j \in J, k \in K\} \subseteq G.$$

## Definition (Quotient group)

Let $G$ be a group and $N \trianglelefteq G$. Equipped with subset multiplication, the set of cosets $G/N$ forms a group: *the quotient group of $G$ by $N$.* The multiplicative structure of cosets on $G/N$ is such that

(1) For every $gN, g'N \in G/N$, $(gN)(g'N) = gg'N$.

(2) The identity of $G/N$ is $N$ itself.

(3) For each $gN \in G/N$, $(gN)^{-1} = g^{-1}N$.

# Quotient groups, intuitively

The elements of quotient groups are sets, which can be difficult to reason about purely by definition. From the perspective of equivalence relations, the quotient group $G/N$ represents a "zoomed out" view of the elements of $G$ once placed into appropriate buckets as determined by some "intrinsic property" of the subgroup $N$, so that almost all differences between elements in the same bucket are "forgotten".

# Quotient groups by example

## Example (Quotients of $\mathbb{Z}$)

It turns out that $m\mathbb{Z} \trianglelefteq \mathbb{Z}$, and so the set of cosets

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

is a quotient group: its elements are sets of integers with the same remainder upon division by $m$. We can therefore identify each coset with this remainder directly, i.e. $\overline{r} \longleftrightarrow r$, and in doing so we are discarding all information except these remainders for each element, and then grouping by remainder.

# A proof involving quotient groups

**2020 Exam, Q1(ii)**

If $N \trianglelefteq G$ and $N \subseteq H \leq G$, show that $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

*Proof.* Let $g \in G$ and $h \in H$.

# A proof involving quotient groups

**2020 Exam, Q1(ii)**

If $N \trianglelefteq G$ and $N \subseteq H \leq G$, show that $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

*Proof.* Let $g \in G$ and $h \in H$. It is clear that $(ghg^{-1})N \in G/N$, and

# A proof involving quotient groups

**2020 Exam, Q1(ii)**

If $N \trianglelefteq G$ and $N \subseteq H \leq G$, show that $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

*Proof.* Let $g \in G$ and $h \in H$. It is clear that $(ghg^{-1})N \in G/N$, and

$$(ghg^{-1})N = (gN)(hN)(g^{-1}N) = (gN)(hN)(gN)^{-1}$$

# A proof involving quotient groups

**2020 Exam, Q1(ii)**

If $N \trianglelefteq G$ and $N \subseteq H \leq G$, show that $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

*Proof.* Let $g \in G$ and $h \in H$. It is clear that $(ghg^{-1})N \in G/N$, and

$$(ghg^{-1})N = (gN)(hN)(g^{-1}N) = (gN)(hN)(gN)^{-1}$$

by the multiplication in $G/N$.

# A proof involving quotient groups

**2020 Exam, Q1(ii)**

If $N \trianglelefteq G$ and $N \subseteq H \leq G$, show that $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

*Proof.* Let $g \in G$ and $h \in H$. It is clear that $(ghg^{-1})N \in G/N$, and

$$(ghg^{-1})N = (gN)(hN)(g^{-1}N) = (gN)(hN)(gN)^{-1}$$

by the multiplication in $G/N$. Now,

$$H \trianglelefteq G \iff ghg^{-1} \in H$$

# A proof involving quotient groups

**2020 Exam, Q1(ii)**

If $N \trianglelefteq G$ and $N \subseteq H \leq G$, show that $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

*Proof.* Let $g \in G$ and $h \in H$. It is clear that $(ghg^{-1})N \in G/N$, and

$$(ghg^{-1})N = (gN)(hN)(g^{-1}N) = (gN)(hN)(gN)^{-1}$$

by the multiplication in $G/N$. Now,

$$H \trianglelefteq G \iff ghg^{-1} \in H \iff (ghg^{-1})N \in H/N$$

# A proof involving quotient groups

**2020 Exam, Q1(ii)**

If $N \trianglelefteq G$ and $N \subseteq H \leq G$, show that $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

*Proof.* Let $g \in G$ and $h \in H$. It is clear that $(ghg^{-1})N \in G/N$, and

$$(ghg^{-1})N = (gN)(hN)(g^{-1}N) = (gN)(hN)(gN)^{-1}$$

by the multiplication in $G/N$. Now,

$$\begin{aligned} H \trianglelefteq G &\iff ghg^{-1} \in H \iff (ghg^{-1})N \in H/N \\ &\iff (gN)(hN)(gN)^{-1} \in H/N \end{aligned}$$

# A proof involving quotient groups

**2020 Exam, Q1(ii)**

If $N \trianglelefteq G$ and $N \subseteq H \leq G$, show that $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

*Proof.* Let $g \in G$ and $h \in H$. It is clear that $(ghg^{-1})N \in G/N$, and

$$(ghg^{-1})N = (gN)(hN)(g^{-1}N) = (gN)(hN)(gN)^{-1}$$

by the multiplication in $G/N$. Now,

$$\begin{aligned} H \trianglelefteq G &\iff ghg^{-1} \in H \iff (ghg^{-1})N \in H/N \\ &\iff (gN)(hN)(gN)^{-1} \in H/N \\ &\iff H/N \trianglelefteq G/N. \end{aligned}$$

# Abelian groups

Before we move on, we introduce an important type of group.

**Definition (Abelian group)**

A group $A$ is said to be *abelian* if $ab = ba$ for all $a, b \in G$. In other words, an abelian group is one in which multiplication is commutative.

# Useful facts about abelian groups

**Theorem**

(1) Every subgroup of an abelian group is abelian and normal.

(2) Every cyclic group is abelian.

(3) A group $G$ is abelian if and only if $(xy)^2 = x^2y^2$.

(4) If $\text{ord}(g) = 2$ for all non-identity $g \in G$, then $G$ is abelian.

# 2. Group Homomorphisms

# Homomorphisms

Though we can define many maps $G \to H$ between groups, those which preserve group structure are of particular interest.

## Definition (Homomorphism)

Let $(G, *)$ and $(H, \bullet)$ be groups. A *group homomorphism* is a map $\phi : G \to H$ that preserves the multiplicative structure of $G$ and $H$, i.e.

$$\phi(g * h) = \phi(g) \bullet \phi(h)$$

for every $g, h \in G$.

As with groups, if the multiplications in $G$ and $H$ are well-understood, we can write $\phi(gh) = \phi(g)\phi(h)$ instead.

# Types of homomorphisms

**Definition (Monomorphism)**

A *monomorphism* is an injective (i.e. 1:1) homomorphism $\phi : G \to H$.

**Definition (Epimorphism)**

An *epimorphism* is a surjective (i.e. onto) homomorphism $\phi : G \to H$.

**Definition (Isomorphism)**

An *isomorphism* is a bijective homomorphism $\phi : G \to H$. In this case, the groups $G$ and $H$ are said to be *isomorphic*, written $G \cong H$.

**Definition (Automorphism)**

An *automorphism* is an isomorphism $\phi : G \to G$.

# Isomorphism

Two groups are isomorphic if there is a complete preservation of their group structure by a mapping from one to the other, short of the elements themselves being equal. From the perspective of group theory, isomorphic groups are thus *indistinguishable*, and it is multiplicative structure that differentiates groups, not elements.

**Example (Isomorphism in dihedral groups)**

The notion of similarity discussed when investigating the subgroups of $D_n$ is precisely isomorphism: $\langle \sigma^k, \sigma^\ell \tau \rangle \cong D_{n/k}$. In other words, the subgroups of $D_n$ are either cyclic or (isomorphically) dihedral.

# Important examples of morphisms

**Example (Quotient morphism)**

If $N \trianglelefteq G$, then the epimorphism $\pi_N : G \to G/N$ defined by $\phi(g) = gN$ is called the *quotient morphism*.

**Example (Inclusion)**

If $H \leq G$, then the monomorphism $\eta : H \hookrightarrow G$ defined by $\eta(h) = h$ is called an *inclusion*. Though simple, inclusions can be helpful when constructing more complicated morphisms.

# Useful facts about morphisms

**Theorem**

Let $\phi : G \to H$ be a homomorphism. Then

(1) $\phi(1_G) = 1_H$ and $\phi(g^{-1}) = (\phi(g))^{-1}$ for all $g \in G$.

(2) $\phi(G') \leq H$ for all $G' \leq G$.

(3) If $\phi$ is an isomorphism, then so is $\phi^{-1} : H \to G$.

(4) If $\phi$ is an isomorphism and $g$ is a generator of $G$, then $\phi(g)$ is a generator of $H$.

(5) If $\psi : H \to K$ is another (compatible) homomorphism, then $\psi \circ \phi : G \to K$ is also homomorphism, and we write $\psi \circ \phi = \psi\phi$.

In addition to this, there are 3 powerful results collectively known as the *isomorphism theorems*. We shall introduce these shortly.

# An example using homomorphisms

## Original example

Let $\phi : G \to \mathbb{C}^*$ be a nontrivial group homomorphism with $G$ finite. Show that

$$\sum_{g \in G} \phi(g) = 0.$$

(Hint: as a coset, $hG = G$ for all $h \in G$.)

*Proof.* Since $\phi$ is nontrivial, there is some $h \in G$ with $\phi(h) \neq 1$, and

# An example using homomorphisms

## Original example

Let $\phi : G \to \mathbb{C}^*$ be a nontrivial group homomorphism with $G$ finite. Show that

$$\sum_{g \in G} \phi(g) = 0.$$

(Hint: as a coset, $hG = G$ for all $h \in G$.)

*Proof.* Since $\phi$ is nontrivial, there is some $h \in G$ with $\phi(h) \neq 1$, and

$$\sum_{g \in G} \phi(g)$$

# An example using homomorphisms

## Original example

Let $\phi : G \to \mathbb{C}^*$ be a nontrivial group homomorphism with $G$ finite. Show that

$$\sum_{g \in G} \phi(g) = 0.$$

(Hint: as a coset, $hG = G$ for all $h \in G$.)

*Proof.* Since $\phi$ is nontrivial, there is some $h \in G$ with $\phi(h) \neq 1$, and

$$\sum_{g \in G} \phi(g) = \sum_{g \in hG} \phi(g)$$

# An example using homomorphisms

## Original example

Let $\phi : G \to \mathbb{C}^*$ be a nontrivial group homomorphism with $G$ finite. Show that

$$\sum_{g \in G} \phi(g) = 0.$$

(Hint: as a coset, $hG = G$ for all $h \in G$.)

*Proof.* Since $\phi$ is nontrivial, there is some $h \in G$ with $\phi(h) \neq 1$, and

$$\sum_{g \in G} \phi(g) = \sum_{g \in hG} \phi(g) = \sum_{g \in G} \phi(hg)$$

# An example using homomorphisms

## Original example

Let $\phi : G \to \mathbb{C}^*$ be a nontrivial group homomorphism with $G$ finite. Show that

$$\sum_{g \in G} \phi(g) = 0.$$

(Hint: as a coset, $hG = G$ for all $h \in G$.)

*Proof.* Since $\phi$ is nontrivial, there is some $h \in G$ with $\phi(h) \neq 1$, and

$$\sum_{g \in G} \phi(g) = \sum_{g \in hG} \phi(g) = \sum_{g \in G} \phi(hg) = \sum_{g \in G} \phi(h)\phi(g)$$

# An example using homomorphisms

## Original example

Let $\phi : G \to \mathbb{C}^*$ be a nontrivial group homomorphism with $G$ finite. Show that

$$\sum_{g \in G} \phi(g) = 0.$$

(Hint: as a coset, $hG = G$ for all $h \in G$.)

*Proof.* Since $\phi$ is nontrivial, there is some $h \in G$ with $\phi(h) \neq 1$, and

$$\sum_{g \in G} \phi(g) = \sum_{g \in hG} \phi(g) = \sum_{g \in G} \phi(hg) = \sum_{g \in G} \phi(h)\phi(g) = \phi(h) \sum_{g \in G} \phi(g).$$

# An example using homomorphisms

## Original example

Let $\phi : G \to \mathbb{C}^*$ be a nontrivial group homomorphism with $G$ finite. Show that

$$\sum_{g \in G} \phi(g) = 0.$$

(Hint: as a coset, $hG = G$ for all $h \in G$.)

*Proof.* Since $\phi$ is nontrivial, there is some $h \in G$ with $\phi(h) \neq 1$, and

$$\sum_{g \in G} \phi(g) = \sum_{g \in hG} \phi(g) = \sum_{g \in G} \phi(hg) = \sum_{g \in G} \phi(h)\phi(g) = \phi(h) \sum_{g \in G} \phi(g).$$

The result follows, since $\phi(h) \neq 1$. □

# Fibres, kernel and image of of homomorphisms

## Definition (Fibre)

Let $\phi : G \to H$ be a group homomorphism and $H' \leq H$. A *fibre of* $\phi$ is

$$\phi^{-1}(H') = \{g \in G : \phi(g) \in H'\}.$$

## Definition (Kernel)

Let $\phi : G \to H$ be a group homomorphism. The *kernel of* $\phi$ is

$$\ker \phi = \phi^{-1}(1_H) = \{g \in G : \phi(g) = 1_H\} \leq G.$$

## Definition (Image)

Let $\phi : G \to H$ be a group homomorphism. The *image of* $\phi$ is

$$\operatorname{im} \phi = \{\phi(g) : g \in G\} \leq H.$$

# Useful facts about kernels

**Theorem**

Let $\phi : G \to H$ be a group homomorphism. Then

(1) $\ker \phi \trianglelefteq G$.

(2) $\phi$ is a monomorphism (i.e. 1:1) if and only if $\ker \phi = 1 = \{1_G\}$.

# A proof involving kernels

**Original example**

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian,

# A proof involving kernels

**Original example**

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian, so $G/H$ is a group.

# A proof involving kernels

## Original example

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian, so $G/H$ is a group. Now, consider the quotient morphism $\pi_H : G \to G/H$.

# A proof involving kernels

**Original example**

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian, so $G/H$ is a group. Now, consider the quotient morphism $\pi_H : G \to G/H$. We know that $\pi_H$ is a homomorphism,

# A proof involving kernels

**Original example**

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian, so $G/H$ is a group. Now, consider the quotient morphism $\pi_H : G \to G/H$. We know that $\pi_H$ is a homomorphism, and that any $g \in \ker \pi_H$ satisfies $gH = H$.

# A proof involving kernels

## Original example

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian, so $G/H$ is a group. Now, consider the quotient morphism $\pi_H : G \to G/H$. We know that $\pi_H$ is a homomorphism, and that any $g \in \ker \pi_H$ satisfies $gH = H$. In particular, this implies that because $1 \in H$,

# A proof involving kernels

## Original example

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian, so $G/H$ is a group. Now, consider the quotient morphism $\pi_H : G \to G/H$. We know that $\pi_H$ is a homomorphism, and that any $g \in \ker \pi_H$ satisfies $gH = H$. In particular, this implies that because $1 \in H$,

$$1 \in gH$$

# A proof involving kernels

**Original example**

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian, so $G/H$ is a group. Now, consider the quotient morphism $\pi_H : G \to G/H$. We know that $\pi_H$ is a homomorphism, and that any $g \in \ker \pi_H$ satisfies $gH = H$. In particular, this implies that because $1 \in H$,

$$1 \in gH \quad \Longrightarrow \quad gh = 1 \text{ for some } h \in H$$

# A proof involving kernels

**Original example**

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian, so $G/H$ is a group. Now, consider the quotient morphism $\pi_H : G \to G/H$. We know that $\pi_H$ is a homomorphism, and that any $g \in \ker \pi_H$ satisfies $gH = H$. In particular, this implies that because $1 \in H$,

$$1 \in gH \quad \Longrightarrow \quad gh = 1 \text{ for some } h \in H \quad \Longrightarrow \quad g = h^{-1},$$

# A proof involving kernels

**Original example**

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian, so $G/H$ is a group. Now, consider the quotient morphism $\pi_H : G \to G/H$. We know that $\pi_H$ is a homomorphism, and that any $g \in \ker \pi_H$ satisfies $gH = H$. In particular, this implies that because $1 \in H$,

$$1 \in gH \quad \Longrightarrow \quad gh = 1 \text{ for some } h \in H \quad \Longrightarrow \quad g = h^{-1},$$

so $g \in H$ too. Thus $\ker \pi_H \subseteq H$,

# A proof involving kernels

## Original example

Let $G$ be an abelian group. Show that every subgroup of $G$ is the kernel of a homomorphism from $G$.

*Proof.* Any $H \leq G$ is normal because $G$ is abelian, so $G/H$ is a group. Now, consider the quotient morphism $\pi_H : G \to G/H$. We know that $\pi_H$ is a homomorphism, and that any $g \in \ker \pi_H$ satisfies $gH = H$. In particular, this implies that because $1 \in H$,

$$1 \in gH \quad \Longrightarrow \quad gh = 1 \text{ for some } h \in H \quad \Longrightarrow \quad g = h^{-1},$$

so $g \in H$ too. Thus $\ker \pi_H \subseteq H$, and the reverse inclusion is clear since $hH = H$ for all $h \in H$, i.e. $\ker \pi_H = H$. $\square$

# First isomorphism theorem

**Theorem (First isomorphism theorem)**

Let $\phi : G \to H$ be a group homomorphism with $K = \ker \phi \trianglelefteq G$. Then $G/K \cong \operatorname{im} \phi$, i.e. there exists an isomorphism $\varphi : G/K \to \operatorname{im} \phi$.

For MATH3711/5706's purposes, this turns out to be the most useful of the three isomorphism theorems. The others are proved using and can be thought of as corollaries of it.

# First isomorphism theorem, intuitively

This theorem is a statement about what needs to be done to transform $\phi$ into an isomorphism:

(1) Force injectivity by considering $\overline{\phi} : G/K \to H$ instead, since we see that if $g \sim g'$, then $g' = gk$ for some $k \in K$, and

$$\phi(g') = \phi(gk) = \phi(g)\phi(k) = \phi(g).$$

That is, any $g'$ with $\phi(g') = \phi(g)$ belongs to the coset $gK$, which are distinct in $G/K$ and thus map to distinct values in $H$ under $\overline{\phi}$.

(2) Force surjectivity by considering the corestriction $\overline{\phi}\big|_{\operatorname{im}\phi}$.

The resulting map $gK \overset{\varphi}{\mapsto} \phi(g)$ is then an isomorphism.

# Using the first isomorphism theorem

## Original example

Prove that there is no nontrivial homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ when $m$ and $n$ are coprime.

*Proof.*

# Using the first isomorphism theorem

## Original example

Prove that there is no nontrivial homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ when $m$ and $n$ are coprime.

*Proof.* Let $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a homomorphism, and let $r = |\operatorname{im} \phi|$.

# Using the first isomorphism theorem

## Original example

Prove that there is no nontrivial homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ when $m$ and $n$ are coprime.

*Proof.* Let $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a homomorphism, and let $r = |\operatorname{im} \phi|$. On one hand, the first isomorphism theorem and Lagrange's theorem together imply that

# Using the first isomorphism theorem

## Original example

Prove that there is no nontrivial homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ when $m$ and $n$ are coprime.

*Proof.* Let $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a homomorphism, and let $r = |\operatorname{im} \phi|$. On one hand, the first isomorphism theorem and Lagrange's theorem together imply that

$$\frac{|\mathbb{Z}/m\mathbb{Z}|}{|\ker \phi|} = r$$

# Using the first isomorphism theorem

## Original example

Prove that there is no nontrivial homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ when $m$ and $n$ are coprime.

*Proof.* Let $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a homomorphism, and let $r = |\operatorname{im} \phi|$. On one hand, the first isomorphism theorem and Lagrange's theorem together imply that

$$\frac{|\mathbb{Z}/m\mathbb{Z}|}{|\ker \phi|} = r \qquad \iff \qquad r \mid m.$$

# Using the first isomorphism theorem

## Original example

Prove that there is no nontrivial homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ when $m$ and $n$ are coprime.

*Proof.* Let $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a homomorphism, and let $r = |\operatorname{im}\phi|$. On one hand, the first isomorphism theorem and Lagrange's theorem together imply that

$$\frac{|\mathbb{Z}/m\mathbb{Z}|}{|\ker\phi|} = r \quad \iff \quad r \mid m.$$

On the other hand, since $\operatorname{im}\phi \leq \mathbb{Z}/n\mathbb{Z}$,

# Using the first isomorphism theorem

## Original example

Prove that there is no nontrivial homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ when $m$ and $n$ are coprime.

*Proof.* Let $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a homomorphism, and let $r = |\operatorname{im}\phi|$. On one hand, the first isomorphism theorem and Lagrange's theorem together imply that

$$\frac{|\mathbb{Z}/m\mathbb{Z}|}{|\ker\phi|} = r \qquad \iff \qquad r \mid m.$$

On the other hand, since $\operatorname{im}\phi \leq \mathbb{Z}/n\mathbb{Z}$, $r \mid n$ by Lagrange's theorem also.

# Using the first isomorphism theorem

## Original example

Prove that there is no nontrivial homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ when $m$ and $n$ are coprime.

*Proof.* Let $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a homomorphism, and let $r = |\operatorname{im}\phi|$. On one hand, the first isomorphism theorem and Lagrange's theorem together imply that

$$\frac{|\mathbb{Z}/m\mathbb{Z}|}{|\ker\phi|} = r \quad \iff \quad r \mid m.$$

On the other hand, since $\operatorname{im}\phi \leq \mathbb{Z}/n\mathbb{Z}$, $r \mid n$ by Lagrange's theorem also. But the only integer that divides coprime integers is 1, so $r = 1$, which is to say that $\phi$ is indeed trivial. □

# Second isomorphism theorem

**Theorem (Second isomorphism theorem)**

Let $G$ be a group, $N, H \trianglelefteq G$ and $N \leq H$. Then $H/N \trianglelefteq G/N$, and

$$\frac{G/N}{H/N} \cong G/H.$$

That is, under the right circumstances, quotienting is cancellative. In other literature, this is sometimes called the third isomorphism theorem.

# Second isomorphism theorem (continued)

The intuition is simple, so this theorem is best illustrated by example.

**Example (Second isomorphism theorem for $\mathbb{Z}$)**

Consider the normal subgroups $n\mathbb{Z}, m\mathbb{Z} \trianglelefteq \mathbb{Z}$. If $n \mid m$, then $n\mathbb{Z} \trianglelefteq m\mathbb{Z}$, and we obtain the isomorphism

$$\frac{\mathbb{Z}/n\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/m\mathbb{Z}.$$

Since these quotient groups essentially act in terms of modular arithmetic, this isomorphism can be interpreted as the fact that reducing modulo $n$ and then by modulo $m$ is equivalent to reducing modulo $m$ in the first place.

# Third isomorphism theorem

**Theorem (Third isomorphism theorem)**

Let $G$ be a group, $N \trianglelefteq G$ and $H \leq G$. Then $HN \leq G$ and $H \cap N \trianglelefteq H$, and moreover

$$\frac{HN}{N} \cong \frac{H}{H \cap N}.$$

In other literature, this is sometimes called the second isomorphism theorem.

# Third isomorphism theorem, intuitively

It would be rational to expect that since $hnH = hH$ for $h \in H$ and $n \in N$, $HN/N$ simply quotients (i.e. filters) out $N$ from $HN$ until just $H$ remains. However, we do not know a priori whether *all* of $H$ survives this process, since if $h \in H \cap N$, then $hnN = N$, and so $H \cap N$ is also quotiented out. Thus, we can at best assume that

$$\frac{HN}{N} \cong \frac{H}{H \cap N}.$$

In the case where $H$ *does* survive entirely (i.e. $H \cap N = 1$), then we recover $HN/N \cong H$. Similarly, in the extreme case where *none* of $H$ survives (i.e. $H \cap N = H$), we have $HN/N \cong 1$.

# Using the third isomorphism theorem

**An adapted example (2006 class test, Q6)**

Given that

$$N := \{\lambda I : \lambda \in \mathbb{C}^*\} \trianglelefteq \mathrm{GL}_n(\mathbb{C}),$$

find a quotient $G$ of $\mathrm{SL}_n(\mathbb{C})$ such that $G \cong \mathrm{GL}_n(\mathbb{C})/N$.

*Solution.* The third isomorphism theorem in this case says that

# Using the third isomorphism theorem

## An adapted example (2006 class test, Q6)

Given that

$$N := \{\lambda I : \lambda \in \mathbb{C}^*\} \trianglelefteq \mathrm{GL}_n(\mathbb{C}),$$

find a quotient $G$ of $\mathrm{SL}_n(\mathbb{C})$ such that $G \cong \mathrm{GL}_n(\mathbb{C})/N$.

*Solution.* The third isomorphism theorem in this case says that

$$\frac{\mathrm{SL}_n(\mathbb{C})N}{N} \cong \frac{\mathrm{SL}_n(\mathbb{C})}{\mathrm{SL}_n(\mathbb{C}) \cap N}.$$

# Using the third isomorphism theorem

**An adapted example (2006 class test, Q6)**

Given that

$$N := \{\lambda I : \lambda \in \mathbb{C}^*\} \trianglelefteq \mathrm{GL}_n(\mathbb{C}),$$

find a quotient $G$ of $\mathrm{SL}_n(\mathbb{C})$ such that $G \cong \mathrm{GL}_n(\mathbb{C})/N$.

*Solution.* The third isomorphism theorem in this case says that

$$\frac{\mathrm{SL}_n(\mathbb{C})N}{N} \cong \frac{\mathrm{SL}_n(\mathbb{C})}{\mathrm{SL}_n(\mathbb{C}) \cap N}.$$

It remains to identify $\mathrm{SL}_n(\mathbb{C})N$ and $\mathrm{SL}_n(\mathbb{C}) \cap N$.

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$.

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$.

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

$$M = MI$$

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

$$M = MI = \left(\lambda^{-1}M\right)(\lambda I),$$

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

$$M = MI = \left(\lambda^{-1}M\right)(\lambda I),$$

so it follows that $\lambda I \in N$

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

$$M = MI = \left(\lambda^{-1}M\right)(\lambda I),$$

so it follows that $\lambda I \in N$ and $\lambda^{-1}M \in \mathrm{SL}_n(\mathbb{C})$, as

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

$$M = MI = \left(\lambda^{-1}M\right)(\lambda I),$$

so it follows that $\lambda I \in N$ and $\lambda^{-1}M \in \mathrm{SL}_n(\mathbb{C})$, as

$$\det(\lambda^{-1}M) = \lambda^{-n}\det M = 1.$$

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

$$M = MI = \left(\lambda^{-1}M\right)(\lambda I),$$

so it follows that $\lambda I \in N$ and $\lambda^{-1}M \in \mathrm{SL}_n(\mathbb{C})$, as

$$\det(\lambda^{-1}M) = \lambda^{-n}\det M = 1.$$

Thus $\mathrm{SL}_n(\mathbb{C})N = \mathrm{GL}_n(\mathbb{C})$. Also, we have

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

$$M = MI = \left(\lambda^{-1}M\right)(\lambda I),$$

so it follows that $\lambda I \in N$ and $\lambda^{-1}M \in \mathrm{SL}_n(\mathbb{C})$, as

$$\det(\lambda^{-1}M) = \lambda^{-n}\det M = 1.$$

Thus $\mathrm{SL}_n(\mathbb{C})N = \mathrm{GL}_n(\mathbb{C})$. Also, we have

$$\mathrm{SL}_n(\mathbb{C}) \cap N =$$

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

$$M = MI = \left(\lambda^{-1}M\right)(\lambda I),$$

so it follows that $\lambda I \in N$ and $\lambda^{-1}M \in \mathrm{SL}_n(\mathbb{C})$, as

$$\det(\lambda^{-1}M) = \lambda^{-n}\det M = 1.$$

Thus $\mathrm{SL}_n(\mathbb{C})N = \mathrm{GL}_n(\mathbb{C})$. Also, we have

$$\mathrm{SL}_n(\mathbb{C}) \cap N = \{\omega I : \det(\omega I) = 1\}$$

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

$$M = MI = \left(\lambda^{-1}M\right)(\lambda I),$$

so it follows that $\lambda I \in N$ and $\lambda^{-1}M \in \mathrm{SL}_n(\mathbb{C})$, as

$$\det(\lambda^{-1}M) = \lambda^{-n}\det M = 1.$$

Thus $\mathrm{SL}_n(\mathbb{C})N = \mathrm{GL}_n(\mathbb{C})$. Also, we have

$$\mathrm{SL}_n(\mathbb{C}) \cap N = \{\omega I : \det(\omega I) = 1\} = \{\omega I : \omega^n = 1\}.$$

# Using the third isomorphism theorem (continued)

It is clear that $\mathrm{SL}_n(\mathbb{C})N \subseteq \mathrm{GL}_n(\mathbb{C})$. To see the reverse inclusion, let $M \in \mathrm{GL}_n(\mathbb{C})$ and $d = \det M \neq 0$. With $\lambda = \sqrt[n]{d} \neq 0$, we have

$$M = MI = \left(\lambda^{-1}M\right)(\lambda I),$$

so it follows that $\lambda I \in N$ and $\lambda^{-1}M \in \mathrm{SL}_n(\mathbb{C})$, as

$$\det(\lambda^{-1}M) = \lambda^{-n}\det M = 1.$$

Thus $\mathrm{SL}_n(\mathbb{C})N = \mathrm{GL}_n(\mathbb{C})$. Also, we have

$$\mathrm{SL}_n(\mathbb{C}) \cap N = \{\omega I : \det(\omega I) = 1\} = \{\omega I : \omega^n = 1\}.$$

The desired quotient is thus $G = \mathrm{SL}_n(\mathbb{C})/\{\omega I : \omega^n = 1\}$.

# 3. Direct Products and Sums

# External direct products

## Definition (External direct product)

Suppose we have groups $G_1$, $G_2$, ..., $G_n$. The Cartesian product of these groups, with the operation of coordinatewise multiplication, is also a group, called the **external direct product** of the groups.

## Quick example

Consider the group $G = (\mathbb{R}^+, *)$. $G \times G$, taken as an external direct product, is simply $\mathbb{R}^+ \times \mathbb{R}^+$. That is, $(2, 3) * (4, 5) = (8, 15)$.

# External direct products

## Definition (Canonical projections and injections)

Two important morphisms associated with the external direct product are the **canonical projection** and the **canonical injection**.

# External direct products

## Definition (Canonical projections and injections)

Two important morphisms associated with the external direct product are the **canonical projection** and the **canonical injection**.

(1) **Canonical projection** $\pi_k : G_1 \times G_2 \times ... \times G_k \times ... \times G_n \to G_k$ such that

$$\pi_k : (g_1, g_2, ..., g_k, ..., g_n) \mapsto g_k.$$

# External direct products

## Definition (Canonical projections and injections)

Two important morphisms associated with the external direct product are the **canonical projection** and the **canonical injection**.

(1) **Canonical projection** $\pi_k : G_1 \times G_2 \times ... \times G_k \times ... \times G_n \to G_k$ such that

$$\pi_k : (g_1, g_2, ..., g_k, ..., g_n) \mapsto g_k.$$

It 'projects' the direct product onto a single group. It is an epimorphism.

# External direct products

## Definition (Canonical projections and injections)

Two important morphisms associated with the external direct product are the **canonical projection** and the **canonical injection**.

(1) **Canonical projection** $\pi_k : G_1 \times G_2 \times ... \times G_k \times ... \times G_n \to G_k$ such that

$$\pi_k : (g_1, g_2, ..., g_k, ..., g_n) \mapsto g_k.$$

It 'projects' the direct product onto a single group. It is an epimorphism.

(2) **Canonical injection** $\iota_k : G_k \to G_1 \times G_2 \times ... \times G_k \times ... \times G_n$ such that

$$\iota_k : g_k \mapsto (1, 1, ..., g_k, ..., 1).$$

# External direct products

## Definition (Canonical projections and injections)

Two important morphisms associated with the external direct product are the **canonical projection** and the **canonical injection**.

(1) **Canonical projection** $\pi_k : G_1 \times G_2 \times ... \times G_k \times ... \times G_n \to G_k$ such that

$$\pi_k : (g_1, g_2, ..., g_k, ..., g_n) \mapsto g_k.$$

It 'projects' the direct product onto a single group. It is an epimorphism.

(2) **Canonical injection** $\iota_k : G_k \to G_1 \times G_2 \times ... \times G_k \times ... \times G_n$ such that

$$\iota_k : g_k \mapsto (1, 1, ..., g_k, ..., 1).$$

It is so named because it is injective (so a monomorphism). We do not 'lose information' through this map, but the non-$k$th coordinates are all set to the identity.

# External direct products

## Quick example

(1) Consider the canonical projection $\pi_2 : \mathbb{R} \times \mathbb{R}^* \times D_6 \times \mathbb{R}^+ \to \mathbb{R}^*$.
$\pi_2(2.6, 3, \tau, 7) =$

# External direct products

## Quick example

(1) Consider the canonical projection $\pi_2 : \mathbb{R} \times \mathbb{R}^* \times D_6 \times \mathbb{R}^+ \to \mathbb{R}^*$. $\pi_2(2.6, 3, \tau, 7) = 3$.

# External direct products

## Quick example

(1) Consider the canonical projection $\pi_2 : \mathbb{R} \times \mathbb{R}^* \times D_6 \times \mathbb{R}^+ \to \mathbb{R}^*$.
$\pi_2(2.6, 3, \tau, 7) = 3$.

(2) Consider the canonical injection $\iota_3 : \mathbb{R}^* \to \mathbb{R}^* \times \mathbb{R} \times \mathbb{R}^* \times S_4$.
$\iota_3(-5) =$

# External direct products

## Quick example

(1) Consider the canonical projection $\pi_2 : \mathbb{R} \times \mathbb{R}^* \times D_6 \times \mathbb{R}^+ \to \mathbb{R}^*$. $\pi_2(2.6, 3, \tau, 7) = 3$.

(2) Consider the canonical injection $\iota_3 : \mathbb{R}^* \to \mathbb{R}^* \times \mathbb{R} \times \mathbb{R}^* \times S_4$. $\iota_3(-5) = (1, 0, -5, (1))$.

# Internal direct products

## Definition (Internal direct product)

Consider groups $G_1, G_2, ..., G_n \leq G$ where

(1) the elements of the different groups commute, but the individual groups are not necessarily abelian, and

(2) for all $i = 1, 2, ..., n$, $G_i \cap (G_1 G_2 ... G_{i-1} G_{i+1} ... G_n) = \{1_G\}$. That is, it is impossible to get any non-identity element in one subgroup from multiplying elements in the other subgroups together.

# Internal direct products

## Definition (Internal direct product)

Consider groups $G_1, G_2, ..., G_n \leq G$ where

(1) the elements of the different groups commute, but the individual groups are not necessarily abelian, and

(2) for all $i = 1, 2, ..., n$, $G_i \cap (G_1 G_2 ... G_{i-1} G_{i+1} ... G_n) = \{1_G\}$. That is, it is impossible to get any non-identity element in one subgroup from multiplying elements in the other subgroups together.

Then the group $G_1 G_2 ... G_n$, termed the **internal direct product**, is isomorphic to the **external direct product** $G_1 \times G_2 \times ... \times G_n$.

# Internal direct products

## Definition (Internal direct product)

Consider groups $G_1, G_2, ..., G_n \leq G$ where

(1) the elements of the different groups commute, but the individual groups are not necessarily abelian, and

(2) for all $i = 1, 2, ..., n$, $G_i \cap (G_1 G_2 ... G_{i-1} G_{i+1} ... G_n) = \{1_G\}$. That is, it is impossible to get any non-identity element in one subgroup from multiplying elements in the other subgroups together.

Then the group $G_1 G_2 ... G_n$, termed the **internal direct product**, is isomorphic to the **external direct product** $G_1 \times G_2 \times ... \times G_n$.

Intuitively, this is because the homomorphism $\phi : G_1 \times G_2 \times ... \times G_n \to G_1 G_2 ... G_n$ where

$$\phi(g_1, g_2, ..., g_n) = g_1 g_2 ... g_n$$

is a bijection.

# Quotients and products of groups

**Theorem**

Interpreting $1 \times H$ as $\{(1_G, h) : h \in H\}$, it is true that

$$(G \times H)/(1 \times H) \cong G.$$

**However**, it is not in general true that $G/H \times H \cong G$.

# Quotients and products of groups

**Theorem**

Interpreting $1 \times H$ as $\{(1_G, h) : h \in H\}$, it is true that

$$(G \times H)/(1 \times H) \cong G.$$

**However**, it is not in general true that $G/H \times H \cong G$.

**(Original example)**

Prove that it is not in general true that

$$G/H \times H \cong G.$$

# Quotients and products of groups

## (Original example)

Prove that it is not in general true that

$$G/H \times H \cong G.$$

## Theorem (for disproving group isomorphism)

Suppose that $G \cong G'$, with isomorphism $\phi : G \to G'$. Then

(1) $|g| = |\phi(g)|$ for all $g \in G$

(2) If $G$ is abelian, then $G'$ is abelian

(3) If $H \leq G$, then $\phi(H) \leq G'$

(4) If $H \trianglelefteq G$, then $\phi(H) \trianglelefteq G'$

# Quotients and products of groups

**(Original example)**

Prove that it is not in general true that

$$G/H \times H \cong G.$$

Take for example the simple finite abelian group $\mathbb{Z}/m\mathbb{Z} \times m\mathbb{Z}$, and compare it with $\mathbb{Z}$.

# Quotients and products of groups

**(Original example)**

Prove that it is not in general true that

$$G/H \times H \cong G.$$

Take for example the simple finite abelian group $\mathbb{Z}/m\mathbb{Z} \times m\mathbb{Z}$, and compare it with $\mathbb{Z}$.

$\mathbb{Z}/m\mathbb{Z} \times m\mathbb{Z}$ has an element of order $m$, that is, $(m\mathbb{Z} + 1, 0)$, whereas none of the elements of $\mathbb{Z}$ have order $m$.

# Quotients and products of groups

**(Original example)**

Prove that it is not in general true that

$$G/H \times H \cong G.$$

Take for example the simple finite abelian group $\mathbb{Z}/m\mathbb{Z} \times m\mathbb{Z}$, and compare it with $\mathbb{Z}$.

$\mathbb{Z}/m\mathbb{Z} \times m\mathbb{Z}$ has an element of order $m$, that is, $(m\mathbb{Z} + 1, 0)$, whereas none of the elements of $\mathbb{Z}$ have order $m$.

So since isomorphisms preserve orders of elements, it cannot be true that $\mathbb{Z}/m\mathbb{Z} \times m\mathbb{Z} \cong \mathbb{Z}$.

Hence, it is not true that in general $G/H \times H \cong G$.

# Direct sums of groups

Recall that in an abelian group, the operation is addition. So the **internal direct product** for abelian groups is called a **direct sum**.

# Direct sums of groups

Recall that in an abelian group, the operation is addition. So the **internal direct product** for abelian groups is called a **direct sum**.

## Theorem

Let $G_1, G_2, ..., G_n$ be subgroups of the abelian group $G$ that generate $G$. Then $G$ is the direct sum of $G_1, G_2, ...,$ and $G_n$ (written as $G = G_1 \oplus G_2 \oplus ... \oplus G_n$) if and only if the only solution to

$$a_1 + a_2 + ... + a_n = 0, \text{ for } a_i \in G_i, i = 1, 2, ..., n$$

is

$$a_1 = a_2 = ... = a_n = 0.$$

# Direct sums of groups

Recall that in an abelian group, the operation is addition. So the **internal direct product** for abelian groups is called a **direct sum**.

## Theorem

Let $G_1, G_2, ..., G_n$ be subgroups of the abelian group $G$ that generate $G$. Then $G$ is the direct sum of $G_1, G_2, ...,$ and $G_n$ (written as $G = G_1 \oplus G_2 \oplus ... \oplus G_n$) if and only if the only solution to

$$a_1 + a_2 + ... + a_n = 0, \text{ for } a_i \in G_i, i = 1, 2, ..., n$$

is

$$a_1 = a_2 = ... = a_n = 0.$$

## (Greenleaf 2014, Question 6.1.18, *adapted*)

Suppose that $A$ and $B$ are abelian groups such that $A \oplus B = G$. Prove that for $a \in A, b \in B$ with finite orders, then $|a + b| = \text{LCM}(|a|, |b|)$.

# Direct sums of groups

(Greenleaf 2014, Question 6.1.18, *adapted*)

Suppose that $A$ and $B$ are abelian groups such that $A \oplus B = G$. Prove that for $a \in A, b \in B$ with finite orders, then $|a+b| = \text{LCM}(|a|, |b|)$.

$|a+b|$ is the smallest positive integer value of $n$ such that $n(a+b) = 0$. But $n(a+b) = na+nb$ by the distributive law, so we need $na+nb = 0$.

# Direct sums of groups

**(Greenleaf 2014, Question 6.1.18, *adapted*)**

Suppose that $A$ and $B$ are abelian groups such that $A \oplus B = G$. Prove that for $a \in A, b \in B$ with finite orders, then $|a+b| = \text{LCM}(|a|, |b|)$.

$|a+b|$ is the smallest positive integer value of $n$ such that $n(a+b) = 0$. But $n(a+b) = na+nb$ by the distributive law, so we need $na+nb = 0$.

So, since $na \in A$ and $nb \in B$, it follows that $na = nb = 0$ as $G$ is the direct sum of $A$ and $B$.

# Direct sums of groups

**(Greenleaf 2014, Question 6.1.18, *adapted*)**

Suppose that $A$ and $B$ are abelian groups such that $A \oplus B = G$. Prove that for $a \in A, b \in B$ with finite orders, then $|a+b| = \text{LCM}(|a|, |b|)$.

$|a+b|$ is the smallest positive integer value of $n$ such that $n(a+b) = 0$. But $n(a+b) = na+nb$ by the distributive law, so we need $na+nb = 0$.

So, since $na \in A$ and $nb \in B$, it follows that $na = nb = 0$ as $G$ is the direct sum of $A$ and $B$.

But for a positive integer $n$, $na = 0$ iff $|a|$ divides $n$, and $nb = 0$ iff $|b|$ divides $n$. Hence, the order of $a+b$ is given by $|a+b| = \text{LCM}(|a|, |b|)$.

# Direct sums of groups

**(Original example)**

Consider the group $G$ generated by $\{x, y, z\}$ with $xyx^{-1}y^{-1} = xzx^{-1}z^{-1} = yzy^{-1}z^{-1} = 1$ and $x^5z = y^3 = 1$. Prove that $G \cong \mathbb{Z} \times \mathbb{Z}/3$, without finding an isomorphism between the two groups.

# Direct sums of groups

**(Original example)**

Consider the group $G$ generated by $\{x, y, z\}$ with $xyx^{-1}y^{-1} = xzx^{-1}z^{-1} = yzy^{-1}z^{-1} = 1$ and $x^5z = y^3 = 1$. Prove that $G \cong \mathbb{Z} \times \mathbb{Z}/3$, without finding an isomorphism between the two groups.

The relations given ($xyx^{-1}y^{-1} = xzx^{-1}z^{-1} = yzy^{-1}z^{-1} = 1$) imply that $x$, $y$, and $z$ all commute, so that $G = \{y^m x^n z^k : m, n, k \in \mathbb{Z}\}$.

# Direct sums of groups

**(Original example)**

Consider the group $G$ generated by $\{x, y, z\}$ with $xyx^{-1}y^{-1} = xzx^{-1}z^{-1} = yzy^{-1}z^{-1} = 1$ and $x^5z = y^3 = 1$. Prove that $G \cong \mathbb{Z} \times \mathbb{Z}/3$, without finding an isomorphism between the two groups.

The relations given ($xyx^{-1}y^{-1} = xzx^{-1}z^{-1} = yzy^{-1}z^{-1} = 1$) imply that $x$, $y$, and $z$ all commute, so that $G = \{y^m x^n z^k : m, n, k \in \mathbb{Z}\}$. But $x^5z = 1$ implies that we can reduce any product of powers of $x$ and $z$ to a power of $x$ as $x^n z^k = x^{n-5k}$, so that $G = \{y^m x^n : m, n \in \mathbb{Z}\}$.

# Direct sums of groups

**(Original example)**

Consider the group $G$ generated by $\{x, y, z\}$ with $xyx^{-1}y^{-1} = xzx^{-1}z^{-1} = yzy^{-1}z^{-1} = 1$ and $x^5z = y^3 = 1$. Prove that $G \cong \mathbb{Z} \times \mathbb{Z}/3$, without finding an isomorphism between the two groups.

The relations given ($xyx^{-1}y^{-1} = xzx^{-1}z^{-1} = yzy^{-1}z^{-1} = 1$) imply that $x$, $y$, and $z$ all commute, so that $G = \{y^m x^n z^k : m, n, k \in \mathbb{Z}\}$. But $x^5z = 1$ implies that we can reduce any product of powers of $x$ and $z$ to a power of $x$ as $x^n z^k = x^{n-5k}$, so that $G = \{y^m x^n : m, n \in \mathbb{Z}\}$.

But we have that $\langle x \rangle \cup \langle y \rangle = 1$ since there are no relations between $x$ and $y$ apart from commutativity. So $G = \langle x \rangle \oplus \langle y \rangle \cong \langle x \rangle \times \langle y \rangle$ by the equivalence of internal and external direct products. But since $y$ has order 3 and $x$ has infinite order, we have then that $G \cong \mathbb{Z} \times \mathbb{Z}/3$.

# Finite abelian groups

It turns out that every finite abelian group is reducible to a direct sum of cyclic groups. Getting to this stage takes a while, though, so we'll first discuss how to classify cyclic groups.

**Theorem (Cyclic groups)**

The only cyclic groups, up to isomorphism, are $\mathbb{Z}$ and $\mathbb{Z}/m$, for $m$ a positive integer.

Note that $\mathbb{Z}$ can be thought of as $\mathbb{Z}/0$, so it is also possible to say that all cyclic groups are $\mathbb{Z}/m$ for an integer $m \geq 0$.

# Finite abelian groups

It turns out that every finite abelian group is reducible to a direct sum of cyclic groups. Getting to this stage takes a while, though, so we'll first discuss how to classify cyclic groups.

## Theorem (Cyclic groups)

The only cyclic groups, up to isomorphism, are $\mathbb{Z}$ and $\mathbb{Z}/m$, for $m$ a positive integer.

Note that $\mathbb{Z}$ can be thought of as $\mathbb{Z}/0$, so it is also possible to say that all cyclic groups are $\mathbb{Z}/m$ for an integer $m \geq 0$.

## Quick example

For instance, the group $\mu_n = \{\omega \in \mathbb{C} : \omega^n = 1\}$ is isomorphic to

# Finite abelian groups

It turns out that every finite abelian group is reducible to a direct sum of cyclic groups. Getting to this stage takes a while, though, so we'll first discuss how to classify cyclic groups.

## Theorem (Cyclic groups)

The only cyclic groups, up to isomorphism, are $\mathbb{Z}$ and $\mathbb{Z}/m$, for $m$ a positive integer.

Note that $\mathbb{Z}$ can be thought of as $\mathbb{Z}/0$, so it is also possible to say that all cyclic groups are $\mathbb{Z}/m$ for an integer $m \geq 0$.

## Quick example

For instance, the group $\mu_n = \{\omega \in \mathbb{C} : \omega^n = 1\}$ is isomorphic to $\boxed{\mathbb{Z}/n}$.

# Finite abelian groups

It turns out that every finite abelian group is reducible to a direct sum of cyclic groups. Getting to this stage takes a while, though, so we'll first discuss how to classify cyclic groups.

## Theorem (Cyclic groups)

The only cyclic groups, up to isomorphism, are $\mathbb{Z}$ and $\mathbb{Z}/m$, for $m$ a positive integer.

Note that $\mathbb{Z}$ can be thought of as $\mathbb{Z}/0$, so it is also possible to say that all cyclic groups are $\mathbb{Z}/m$ for an integer $m \geq 0$.

## Quick example

For instance, the group $\mu_n = \{\omega \in \mathbb{C} : \omega^n = 1\}$ is isomorphic to $\boxed{\mathbb{Z}/n}$.

The group $\{2^n : n \in \mathbb{Z}\} \leq (\mathbb{R}^+, *)$ is isomorphic to

# Finite abelian groups

It turns out that every finite abelian group is reducible to a direct sum of cyclic groups. Getting to this stage takes a while, though, so we'll first discuss how to classify cyclic groups.

## Theorem (Cyclic groups)

The only cyclic groups, up to isomorphism, are $\mathbb{Z}$ and $\mathbb{Z}/m$, for $m$ a positive integer.

Note that $\mathbb{Z}$ can be thought of as $\mathbb{Z}/0$, so it is also possible to say that all cyclic groups are $\mathbb{Z}/m$ for an integer $m \geq 0$.

## Quick example

For instance, the group $\mu_n = \{\omega \in \mathbb{C} : \omega^n = 1\}$ is isomorphic to $\boxed{\mathbb{Z}/n}$.

The group $\{2^n : n \in \mathbb{Z}\} \leq (\mathbb{R}^+, *)$ is isomorphic to $\boxed{\mathbb{Z}}$.

# Finite abelian groups

The first step to breaking finite abelian groups down is to break them down into generating subgroups called $p$-parts.

## Definition ($p$-parts)

Consider a prime $p$ and a finite abelian group $A$. The $p$-part of $G$, written $A_p$, is the set of elements of $A$ whose order is a power of $p$. That is,

$$A_p = \{a \in A : p^n a = 0 \text{ for some } n \geq 1\}.$$

The $p$-part of $A$ is a subgroup of $A$.

# Finite abelian groups

The first step to breaking finite abelian groups down is to break them down into generating subgroups called $p$-parts.

## Definition ($p$-parts)

Consider a prime $p$ and a finite abelian group $A$. The $p$-part of $G$, written $A_p$, is the set of elements of $A$ whose order is a power of $p$. That is,

$$A_p = \{a \in A : p^n a = 0 \text{ for some } n \geq 1\}.$$

The $p$-part of $A$ is a subgroup of $A$.

## Theorem (Decomposition of $A$ into $p$-parts)

Let $A$ be a finite abelian group, and let the prime factors of $|A|$ be $p_1, p_2, ..., p_n$. Then

$$A = A_{p_1} \oplus A_{p_2} \oplus ... \oplus A_{p_n}.$$

# Finite abelian groups

Okay, so we've established so far that a finite abelian group can be decomposed into a direct sum of its $p$-parts. But the real magic happens when we decompose the $p$-parts further:

# Finite abelian groups

Okay, so we've established so far that a finite abelian group can be decomposed into a direct sum of its $p$-parts. But the real magic happens when we decompose the $p$-parts further:

**Theorem (Decomposition of $p$-parts into cyclic groups)**

Consider $G = A_p$, that is, the $p$-part of some finite abelian group $A$. We can write $G$ as the direct sum of cyclic groups of order $p^n$, that is,

$$\begin{aligned} G &= \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus ... \oplus \langle a_k \rangle \\ &\cong \boxed{\mathbb{Z}/p^{n_1} \oplus \mathbb{Z}/p^{n_2} \oplus ... \oplus \mathbb{Z}/p^{n_k}} \end{aligned}$$

for positive integers $n_1, n_2, ...n_k \geq 1$.

# Finite abelian groups

Okay, so we've established so far that a finite abelian group can be decomposed into a direct sum of its $p$-parts. But the real magic happens when we decompose the $p$-parts further:

**Theorem (Decomposition of $p$-parts into cyclic groups)**

Consider $G = A_p$, that is, the $p$-part of some finite abelian group $A$. We can write $G$ as the direct sum of cyclic groups of order $p^n$, that is,

$$\begin{aligned} G &= \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus ... \oplus \langle a_k \rangle \\ &\cong \boxed{\mathbb{Z}/p^{n_1} \oplus \mathbb{Z}/p^{n_2} \oplus ... \oplus \mathbb{Z}/p^{n_k}} \end{aligned}$$

for positive integers $n_1, n_2, ...n_k \geq 1$.

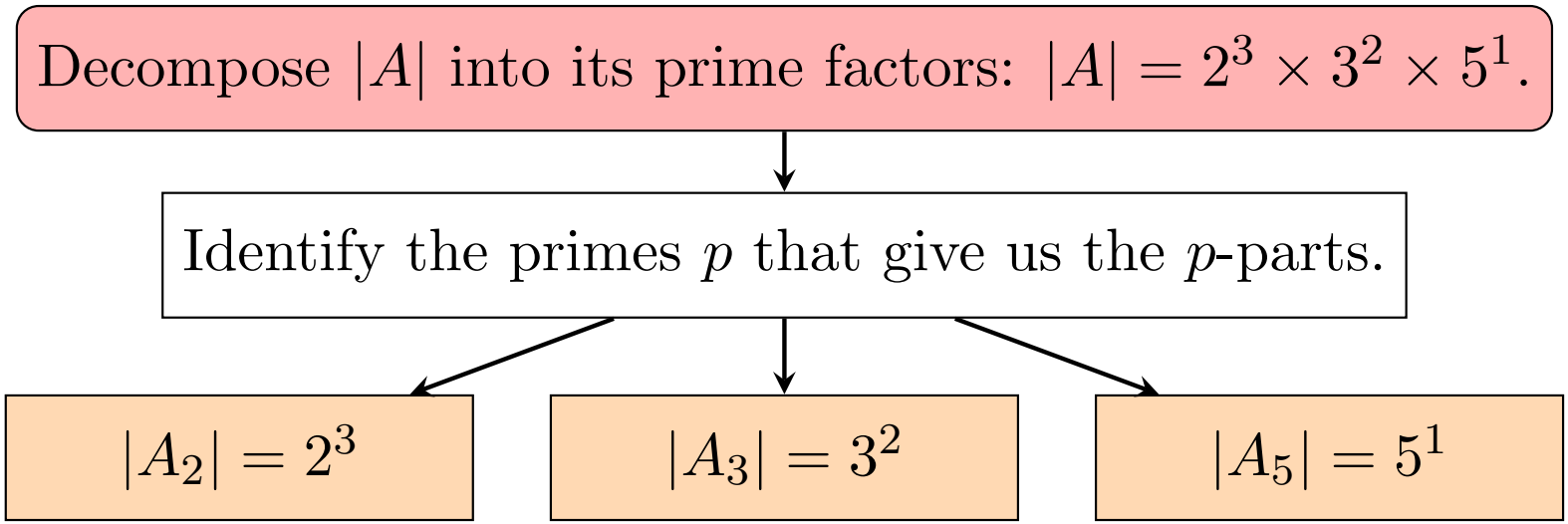
Also, for a given group, the orders of the individual cyclic groups must always be the same (up to ordering). That also means that groups with different orders in their cyclic decompositions must not be isomorphic.

# Finite abelian groups: Putting it all together

For instance, how might we use this to find all the finite abelian groups of order 360 up to isomorphism?

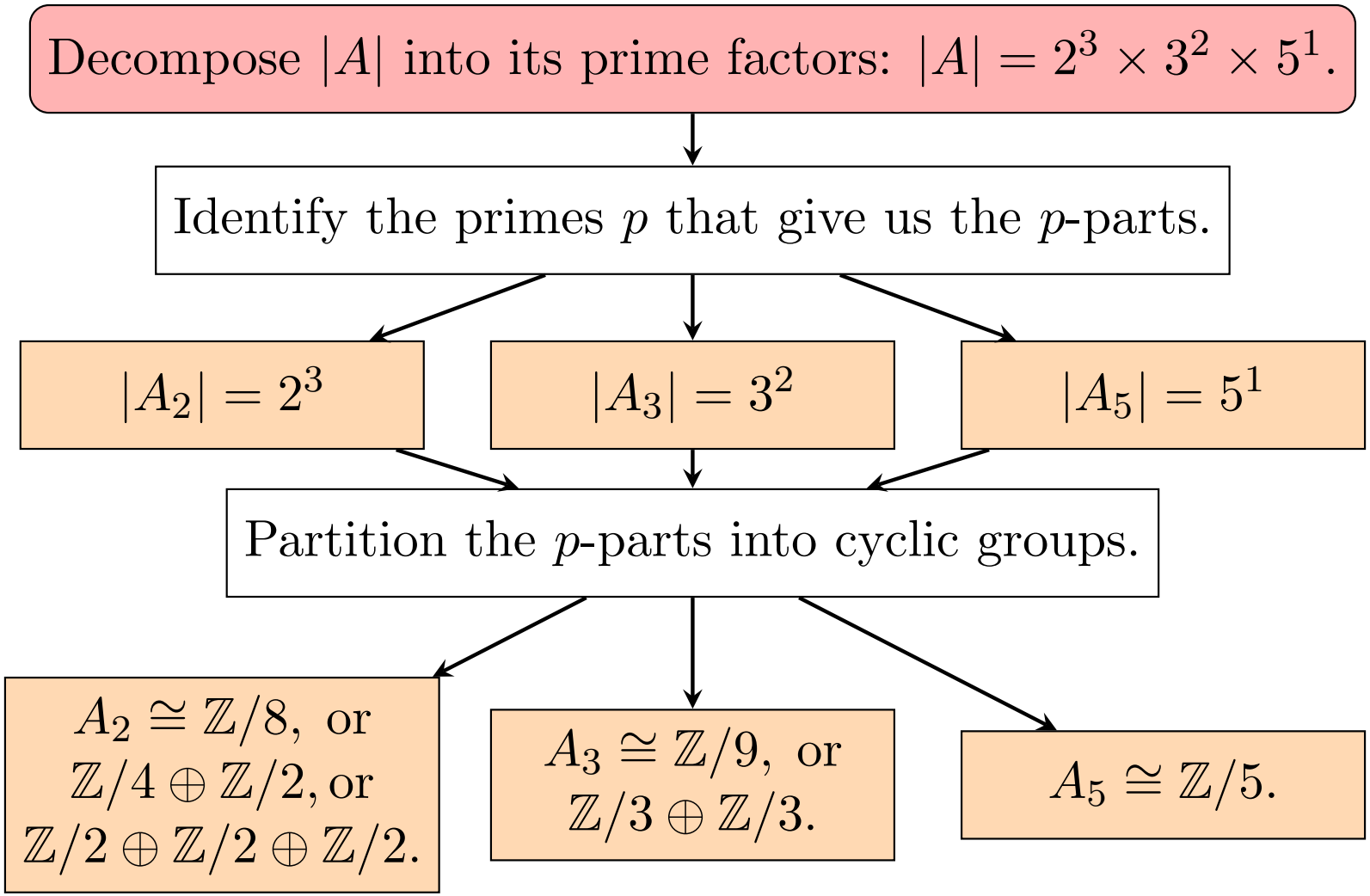
# Finite abelian groups: Putting it all together

For instance, how might we use this to find all the finite abelian groups of order 360 up to isomorphism?



# Finite abelian groups: Putting it all together

For instance, how might we use this to find all the finite abelian groups of order 360 up to isomorphism?



# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

A natural condition to start off with is $\gcd(n, d) = 1$.

# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

A natural condition to start off with is $\gcd(n, d) = 1$. We want to show somehow that if $\gcd(n, d) \neq 1$, then $\phi_d(x) = dx$ is not an isomorphism. We also want to show the converse, that is, that if $\gcd(n, d) = 1$, then $\phi_d(x) = dx$ is an isomorphism.

# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

A natural condition to start off with is $\gcd(n, d) = 1$. We want to show somehow that if $\gcd(n, d) \neq 1$, then $\phi_d(x) = dx$ is not an isomorphism. We also want to show the converse, that is, that if $\gcd(n, d) = 1$, then $\phi_d(x) = dx$ is an isomorphism.

Now, since $\phi_d$ maps between finite abelian groups of the same order, it is bijective if and only if $\ker(\phi_d) = \{0\}$, that is, if and only if there is no element whose order is a factor of $d$.

# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

But G can be written as a non-trivial direct sum of its $p$-parts, that is, $G = A_{p_1} \oplus A_{p_2} \oplus ... \oplus A_{p_i}$ for $p_1, p_2, ..., p_i$ the prime factors of $n$.

# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

But G can be written as a non-trivial direct sum of its $p$-parts, that is, $G = A_{p_1} \oplus A_{p_2} \oplus ... \oplus A_{p_i}$ for $p_1, p_2, ..., p_i$ the prime factors of $n$.

Consider any prime factor of $n$, $p_i$.

# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

But G can be written as a non-trivial direct sum of its $p$-parts, that is, $G = A_{p_1} \oplus A_{p_2} \oplus ... \oplus A_{p_i}$ for $p_1, p_2, ..., p_i$ the prime factors of $n$.

Consider any prime factor of $n$, $p_i$. There must exist in $A_{p_i}$ some element $g$ of order $p_i^k$ for $k \geq 1$. Then, $p_i^{k-1}g$ must have order $p_i$, showing the existence of an element of order $p_i$.

# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

But G can be written as a non-trivial direct sum of its $p$-parts, that is, $G = A_{p_1} \oplus A_{p_2} \oplus ... \oplus A_{p_i}$ for $p_1, p_2, ..., p_i$ the prime factors of $n$.

Consider any prime factor of $n$, $p_i$. There must exist in $A_{p_i}$ some element $g$ of order $p_i^k$ for $k \geq 1$. Then, $p_i^{k-1}g$ must have order $p_i$, showing the existence of an element of order $p_i$. So if $d$ shares any factors with $n$, then we can pick a prime factor $p$ that they have in common and find an element with order $p$ which divides $d$. Hence, if $d$ shares any factors with $n$, the kernel of $\phi_d$ cannot be trivial.

# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

But we also need to show that if $\gcd(n, d) = 1$, $\phi_d$ is an isomorphism.

# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

But we also need to show that if $\gcd(n, d) = 1$, $\phi_d$ is an isomorphism.

So suppose that $\gcd(n, d) = 1$.

# Finite abelian groups: Putting it all together

**(2018, Question 2 d)**

Assume that $G$ is a finite abelian group of order $n$ for some positive integer $n$. Determine for which positive integers $d$ the map $\phi_d : G \to G, \phi_d(x) = dx$ is an isomorphism. Your criterion should be a simple condition involving the integers $n$ and $d$. Prove that your criterion is correct.

But we also need to show that if $\gcd(n, d) = 1$, $\phi_d$ is an isomorphism.

So suppose that $\gcd(n, d) = 1$. The orders of all the elements of $G$ must divide $n$, so if we want the order of an element to divide $d$, it follows that the order must be 1. Hence, if $\gcd(n, d) = 1$, then the kernel of $\phi_d$ is trivial, and $\phi_d$ is an isomorphism. So we have successfully shown that our condition is necessary **and** sufficient!

# Finite abelian groups: Putting it all together

**(Additional example)**

Prove that a finite abelian group is cyclic if and only if all of its $p$-parts are cyclic.

# Finite abelian groups: Putting it all together

**(Additional example)**

Prove that a finite abelian group is cyclic if and only if all of its $p$-parts are cyclic.

Left as an exercise!

# 4. Group Actions

# The group $O_n$

## Definition ($\mathrm{Isom}(\mathbb{R}^n)$)

$\mathrm{Isom}(\mathbb{R}^n) \leq \mathrm{Perm}(\mathbb{R}^n)$ is defined as the set of all isometries, that is, functions satisfying $\|T(\mathbf{x}) - T(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\|$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. All isometries are in the form

$$T(\mathbf{v}) = Q\mathbf{v} + \mathbf{c}$$

for some orthogonal $Q$ and some vector $\mathbf{c} \in \mathbb{R}^n$.

# The group $O_n$

## Definition ($\mathrm{Isom}(\mathbb{R}^n)$)

$\mathrm{Isom}(\mathbb{R}^n) \leq \mathrm{Perm}(\mathbb{R}^n)$ is defined as the set of all isometries, that is, functions satisfying $\|T(\mathbf{x}) - T(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\|$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. All isometries are in the form

$$T(\mathbf{v}) = Q\mathbf{v} + \mathbf{c}$$

for some orthogonal $Q$ and some vector $\mathbf{c} \in \mathbb{R}^n$.

## Definition ($O_n$)

$O_n = O(\mathbb{R}^n)$ is defined as the set of all isometries that fix the point $\mathbf{0}$. It is essentially the set of orthogonal matrices in $GL_n$, since we have wiped out the constant term in the general form $T(\mathbf{v}) = Q\mathbf{v} + \mathbf{c}$.

# The group $O_2$

**Theorem**

Every subgroup of $O_2$ is isomorphic to either the group of rotational symmetries of an $n$-gon (the cyclic group $C_n$) or the group of all symmetries of an $n$-gon (the dihedral group $D_n$).

# The group $O_2$

**Theorem**

Every subgroup of $O_2$ is isomorphic to either the group of rotational symmetries of an $n$-gon (the cyclic group $C_n$) or the group of all symmetries of an $n$-gon (the dihedral group $D_n$).

**Original example**

Consider the hexagon that consists of a square with two equilateral triangles lying on opposite edges. Explain why the group of symmetries of this shape is isomorphic to a subgroup of $O_2$, and identify the group of symmetries of this shape up to isomorphism.

# The group $O_2$

**Original example**

Consider the hexagon that consists of a square with two equilateral triangles lying on opposite edges. Explain why the group of symmetries of this shape is isomorphic to a subgroup of $O_2$, and identify the cyclic or dihedral group that it is isomorphic to.

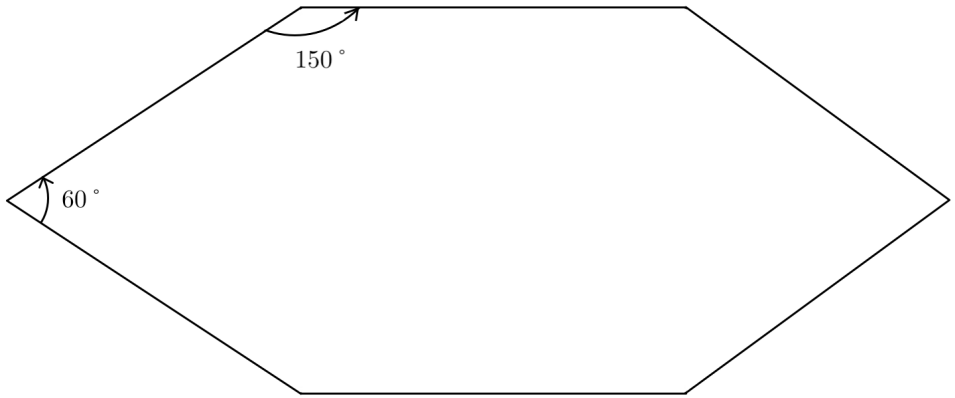
Since this is a finite subgroup of $\text{Isom}(\mathbb{R}^2)$, it must be isomorphic to a subgroup of $O_2$.

# The group $O_2$

## Original example

Consider the hexagon that consists of a square with two equilateral triangles lying on opposite edges. Explain why the group of symmetries of this shape is isomorphic to a subgroup of $O_2$, and identify the cyclic or dihedral group that it is isomorphic to.

Since this is a finite subgroup of $\mathrm{Isom}(\mathbb{R}^2)$, it must be isomorphic to a subgroup of $O_2$.



# The group $O_2$

**Original example**

Consider the hexagon that consists of a square with two equilateral triangles lying on opposite edges. Explain why the group of symmetries of this shape is isomorphic to a subgroup of $O_2$, and identify the cyclic or dihedral group that it is isomorphic to.

Since this is a finite subgroup of $\text{Isom}(\mathbb{R}^2)$, it must be isomorphic to a subgroup of $O_2$. There is one identity in this group, exactly one $180°$ rotation that preserves the orientation of the hexagon, and exactly two reflections that preserve the orientation of the hexagon.

# The group $O_2$

## Original example

Consider the hexagon that consists of a square with two equilateral triangles lying on opposite edges. Explain why the group of symmetries of this shape is isomorphic to a subgroup of $O_2$, and identify the cyclic or dihedral group that it is isomorphic to.

Since this is a finite subgroup of $\text{Isom}(\mathbb{R}^2)$, it must be isomorphic to a subgroup of $O_2$. There is one identity in this group, exactly one $180°$ rotation that preserves the orientation of the hexagon, and exactly two reflections that preserve the orientation of the hexagon.

This is exactly the structure of $D_2$.

# $O_3$ and the special orthogonal group $SO_3$

**Definition ($SO_n$)**

An example of an infinite subgroup of the orthogonal group $O_n$ is the **special orthogonal group** $SO_n$, which is the group of all orthogonal matrices with determinant 1.

# $O_3$ and the special orthogonal group $SO_3$

## Definition ($SO_n$)

An example of an infinite subgroup of the orthogonal group $O_n$ is the **special orthogonal group** $SO_n$, which is the group of all orthogonal matrices with determinant 1.

## The group $SO_3$

By extension, $SO_3$ is the special orthogonal group of dimension 3. It is the group of rotations in $\mathbb{R}^3$.

# $O_3$ and the special orthogonal group $SO_3$

It turns out that we can classify the finite subgroups of $SO_3$ into a number of simple categories.

**Theorem (Finite subgroups of $SO_3$)**

Any subgroup of $SO_3$ must be one of the following:

(1) A cyclic group $C_n$ (rotations by $\frac{2\pi}{n}$ along a given plane)

# $O_3$ and the special orthogonal group $SO_3$

It turns out that we can classify the finite subgroups of $SO_3$ into a number of simple categories.

**Theorem (Finite subgroups of $SO_3$)**

Any subgroup of $SO_3$ must be one of the following:

(1) A cyclic group $C_n$ (rotations by $\frac{2\pi}{n}$ along a given plane)

(2) A dihedral group $D_n$ (rotations by $\frac{2\pi}{n}$ along a given plane, along with a rotation flipping the plane)

# $O_3$ and the special orthogonal group $SO_3$

It turns out that we can classify the finite subgroups of $SO_3$ into a number of simple categories.

**Theorem (Finite subgroups of $SO_3$)**

Any subgroup of $SO_3$ must be one of the following:

(1) A cyclic group $C_n$ (rotations by $\frac{2\pi}{n}$ along a given plane)

(2) A dihedral group $D_n$ (rotations by $\frac{2\pi}{n}$ along a given plane, along with a rotation flipping the plane)

(3) The group of rotational symmetries of a Platonic solid (tetrahedron, cube/octahedron, icosahedron/dodecahedron)

# Rotational symmetries of Platonic solids

How do we classify these rotational symmetry groups?

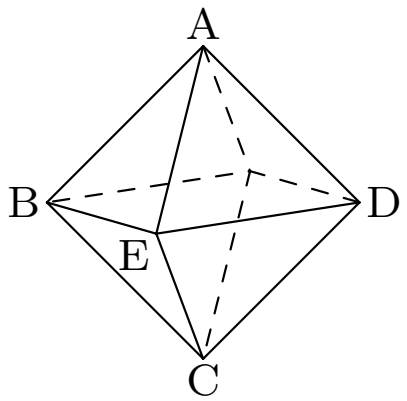
# Rotational symmetries of Platonic solids

How do we classify these rotational symmetry groups?

**Theorem (Sizes of rotational symmetry groups)**

The rotational symmetry group of a Platonic solid has size equal to

$$|G| = \text{Number of faces} \times \text{Number of edges on each face.}$$



# Rotational symmetries of Platonic solids

How do we classify these rotational symmetry groups?

**Theorem (Understanding these rotational symmetry groups)**

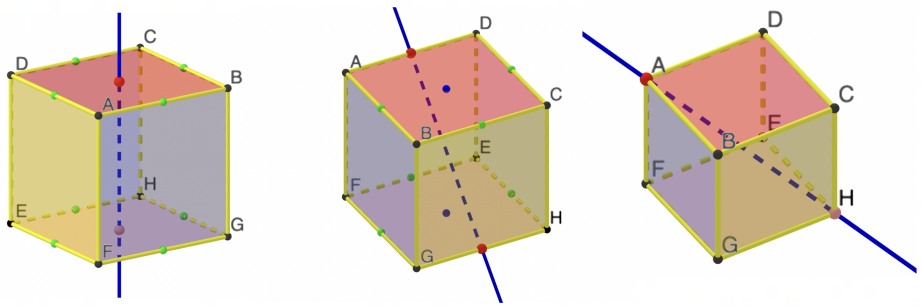
The elements of these rotational symmetry groups consist of

(1) The identity transformation

(2) Rotations about an axis joining the midpoints of opposite edges

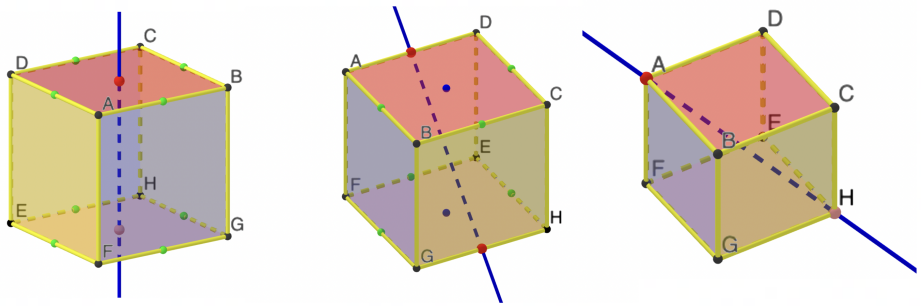
(3) Rotations about an axis joining opposite vertices

(4) Rotations about an axis joining the midpoints of opposite faces



# Rotational symmetries of Platonic solids

How do we classify these rotational symmetry groups?



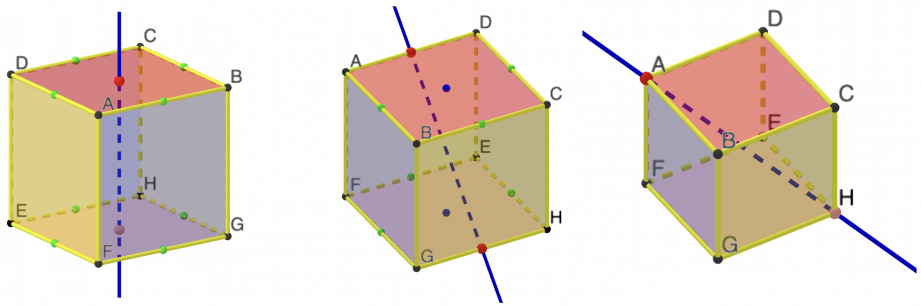

## Rotational symmetries of a cube

For instance, for the rotational symmetries of a cube, we have

(1) The identity transformation - **1**

# Rotational symmetries of Platonic solids

How do we classify these rotational symmetry groups?




## Rotational symmetries of a cube

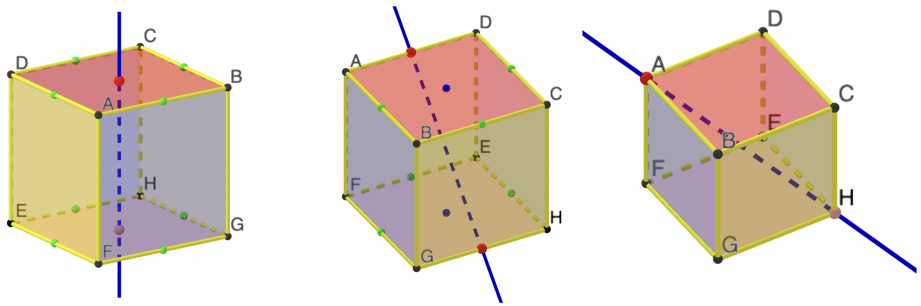
For instance, for the rotational symmetries of a cube, we have

(1) The identity transformation - **1**

(2) Rotations about an axis joining the midpoints of opposite edges - $\mathbf{6 \times 1}$

# Rotational symmetries of Platonic solids

How do we classify these rotational symmetry groups?




## Rotational symmetries of a cube

For instance, for the rotational symmetries of a cube, we have

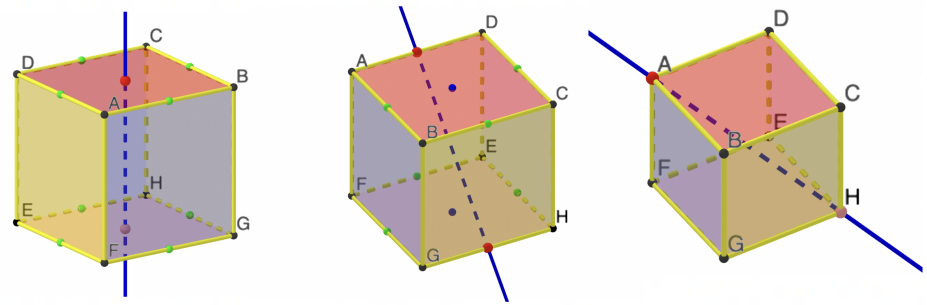
(1) The identity transformation - **1**

(2) Rotations about an axis joining the midpoints of opposite edges - $\mathbf{6 \times 1}$

(3) Rotations about an axis joining opposite vertices - $\mathbf{4 \times 2}$

# Rotational symmetries of Platonic solids

How do we classify these rotational symmetry groups?




## Rotational symmetries of a cube

For instance, for the rotational symmetries of a cube, we have

(1) The identity transformation - **1**

(2) Rotations about an axis joining the midpoints of opposite edges - $\mathbf{6 \times 1}$

(3) Rotations about an axis joining opposite vertices - $\mathbf{4 \times 2}$

(4) Rotations about an axis joining the midpoints of opposite faces - $\mathbf{3 \times 3}$

# $G$-sets and group actions

We can start to think about a group 'acting' on elements in a given set.

## Definition ($G$-set)

Suppose we have a set $S$, and we define a map $\alpha : G \times S \to S$ (where we can define $\alpha(g, s) := g.s$). Then we can say that $G$ acts on the set $S$, so long as the following conditions hold:

(1) $(gh).s = g.(h.s)$ for all $g, h \in G$ and $s \in S$.

(2) $1_G.s = s$ for all $s \in S$

The set together with the operation is called a $G$-set.

We can think of this as a group homomorphism from $G$ to $\mathrm{Perm}(S)$, since for each element of $G$ we define an invertible action from $S$ to itself.

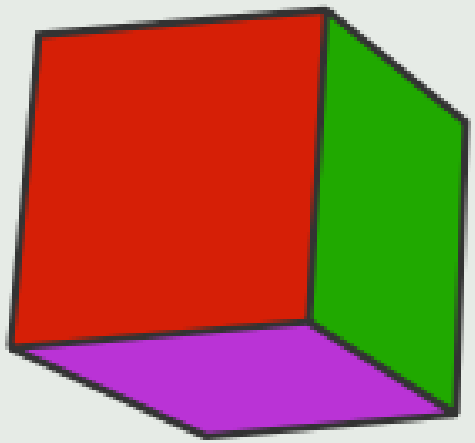
# $G$-sets and group actions

## Examples ($G$-sets)

(1) A simple example is the group of unit scalars $\mathbb{R}^*$ acting on any vector space over $\mathbb{R}$

(2) The group of symmetries of a Platonic solid can act on arrangements/colourings of the Platonic solid

(3) The set $G/H$ is a $G$-set under the group action $g'.gH = (g'g)H$



# Orbits

**Definition ($G$-stable subsets)**

A subset $T \subseteq S$ is $G$-stable if $G.T \subseteq T$.

# Orbits

**Definition ($G$-stable subsets)**

A subset $T \subseteq S$ is $G$-stable if $G.T \subseteq T$.

**Definition (Orbit)**

The orbit of $s \in S$ is the subset $G.s$. It is the smallest $G$-stable subset of $S$ that contains $s$. It can be thought of as all the elements of $S$ that one can 'get to' from acting on $s$.

# Orbits

**Definition ($G$-stable subsets)**

A subset $T \subseteq S$ is $G$-stable if $G.T \subseteq T$.

**Definition (Orbit)**

The orbit of $s \in S$ is the subset $G.s$. It is the smallest $G$-stable subset of $S$ that contains $s$. It can be thought of as all the elements of $S$ that one can 'get to' from acting on $s$.

**Example**

For instance, what are the orbits of $\mathbb{R}^n$ under $O_n$?

# Orbits

**Definition ($G$-stable subsets)**

A subset $T \subseteq S$ is $G$-stable if $G.T \subseteq T$.

**Definition (Orbit)**

The orbit of $s \in S$ is the subset $G.s$. It is the smallest $G$-stable subset of $S$ that contains $s$. It can be thought of as all the elements of $S$ that one can 'get to' from acting on $s$.

**Example**

For instance, what are the orbits of $\mathbb{R}^n$ under $O_n$? What are the orbits of $G/H$ when equipped with the standard group action under $G$?

# Orbits

**Theorem (Orbit structures)**

If we define the relation $\sim$ as $s \sim s'$ if and only if $s \in G.s'$, then $\sim$ is an equivalence relation. Therefore, the $G$-orbits of a set partition a set into disjoint subsets.

# Orbits

**Theorem (Orbit structures)**

If we define the relation $\sim$ as $s \sim s'$ if and only if $s \in G.s'$, then $\sim$ is an equivalence relation. Therefore, the $G$-orbits of a set partition a set into disjoint subsets.

**Definition (Transitive action)**

A group $G$ acts transitively on a set $S$ if $S$ consists of only one orbit.

# Orbits

**Theorem (Orbit structures)**

If we define the relation $\sim$ as $s \sim s'$ if and only if $s \in G.s'$, then $\sim$ is an equivalence relation. Therefore, the $G$-orbits of a set partition a set into disjoint subsets.

**Definition (Transitive action)**

A group $G$ acts transitively on a set $S$ if $S$ consists of only one orbit.

**Example (Conjugacy classes)**

$G$ acts on $G$ by conjugation, where conjugation is the map such that $g_1.g_2 = g_1 g_2 g_1^{-1}$. The orbits of $G$ under this group action are called **conjugacy classes**.

# Orbits

**(2016, Question 1 b)**

List the conjugacy classes of the symmetric group $S_4$, by giving a representative element for each class. (You do not need to write down every element in each class.)

Simply go through the elements of $S_4$ and attempt to partition them.

# Orbits

**(2016, Question 1 b)**

List the conjugacy classes of the symmetric group $S_4$, by giving a representative element for each class. (You do not need to write down every element in each class.)

Simply go through the elements of $S_4$ and attempt to partition them.

$\{(1)\}$.

# Orbits

**(2016, Question 1 b)**

List the conjugacy classes of the symmetric group $S_4$, by giving a representative element for each class. (You do not need to write down every element in each class.)

Simply go through the elements of $S_4$ and attempt to partition them.

$\{(1)\}$.

$\{(12)$,

# Orbits

**(2016, Question 1 b)**

List the conjugacy classes of the symmetric group $S_4$, by giving a representative element for each class. (You do not need to write down every element in each class.)

Simply go through the elements of $S_4$ and attempt to partition them.

$\{(1)\}$.

$\{(12), (13), (14), (23), (24), (34)\}$.

# Orbits

**(2016, Question 1 b)**

List the conjugacy classes of the symmetric group $S_4$, by giving a representative element for each class. (You do not need to write down every element in each class.)

Simply go through the elements of $S_4$ and attempt to partition them.

$\{(1)\}$.

$\{(12), (13), (14), (23), (24), (34)\}$.

$\{(123), (124), (134), (234), ...\}$.

# Orbits

**(2016, Question 1 b)**

List the conjugacy classes of the symmetric group $S_4$, by giving a representative element for each class. (You do not need to write down every element in each class.)

Simply go through the elements of $S_4$ and attempt to partition them.

$\{(1)\}$.

$\{(12), (13), (14), (23), (24), (34)\}$.

$\{(123), (124), (134), (234), ...\}$.

$\{(1234), (1324), ...\}$.

# $G$-set morphisms

## Isomorphism of $G$-sets

For two $G$-sets $S_1$ and $S_2$, a $G$-set morphism is a function $\psi : S_1 \to S_2$ such that

$$\psi(g.s) = g.\psi(s) \text{ for all } g \in G, s \in S.$$

$\psi$ is then called compatible with the group action, or $G$-equivariant.

If $\psi$ is bijective, then the $G$-sets $S_1$ and $S_2$ are isomorphic.

# Stabilisers

## Definition (Stabilisers)

For $S$ a $G$-set, the stabiliser of the element $s \in S$ is the subgroup

$$\mathrm{stab}_G(s) = \{g \in G : g.s = s\}.$$

That is, it is the subgroup of all elements $g$ that fix $s \in S$.

## Examples

For example, what are the stabilisers of $gH$ in $G/H$ under the standard $G$-action?

# Orbit-stabiliser theorem

**Theorem (Orbit-stabiliser theorem)**

Given a $G$-set $S$ and an element $s \in S$, the map

$$\phi : G.s \to G/\text{stab}_G(s) \text{ such that } \phi(g.s) = g\text{stab}_G(s)$$

is a $G$-set isomorphism. Thus, $G.s \cong G/\text{stab}_G(s)$.

**Corollary**

For a $G$-set $S$ and an element $s \in S$, $|G.s| = |G|/|\text{stab}_G(s)|$. That is,

$$\text{Size of stabiliser} \times \text{Size of orbit} = \text{Order of group}.$$

# Orbit-stabiliser theorem

## Original example

Let $H$ and $K$ be two subgroups of the finite group $G$. $H \times K$ acts on $HK$ according to the map

$$(h_1, k_1).hk = h_1 hk k_1^{-1} \text{ for all } h, h_1 \in H, k, k_1 \in K.$$

Use the orbit-stabiliser theorem to show that

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

We want to be using the theorem $|G.s| = |G|/|\text{stab}_G(s)|$. To do this, we need to identify our group $H \times K$ and our set $HK$.

We also need to identify a suitable element to calculate the orbit of.

# Orbit-stabiliser theorem

## Original example

Let $H$ and $K$ be two subgroups of the finite group $G$. $H \times K$ acts on $HK$ according to the map

$$(h_1, k_1).hk = h_1 hk k_1^{-1} \text{ for all } h, h_1 \in H, k, k_1 \in K.$$

Use the orbit-stabiliser theorem to show that

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

Now the stabiliser of $1_G$ is the set

$$\text{stab}_G(1_G) = \{(h_1, k_1) \in H \times K : h_1 k_1^{-1} = 1_G\},$$

# Orbit-stabiliser theorem

## Original example

Let $H$ and $K$ be two subgroups of the finite group $G$. $H \times K$ acts on $HK$ according to the map

$$(h_1, k_1).hk = h_1 hk k_1^{-1} \text{ for all } h, h_1 \in H, k, k_1 \in K.$$

Use the orbit-stabiliser theorem to show that

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

Now the stabiliser of $1_G$ is the set

$$\text{stab}_G(1_G) = \{(h_1, k_1) \in H \times K : h_1 k_1^{-1} = 1_G\},$$

which is simply $\{(h_1, h_1) \in H \times K : h_1 \in H \cap K\}$ and has size $|H \cap K|$.

# Orbit-stabiliser theorem

## Original example

Let $H$ and $K$ be two subgroups of the finite group $G$. $H \times K$ acts on $HK$ according to the map

$$(h_1, k_1).hk = h_1 hk k_1^{-1} \text{ for all } h, h_1 \in H, k, k_1 \in K.$$

Use the orbit-stabiliser theorem to show that

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

Now we calculate the orbit of $1_G$. The orbit of the set, by definition, is

$$(H \times K).1_G = \{h_1 k_1^{-1} : h_1 \in H, k_1 \in K\},$$

# Orbit-stabiliser theorem

## Original example

Let $H$ and $K$ be two subgroups of the finite group $G$. $H \times K$ acts on $HK$ according to the map

$$(h_1, k_1).hk = h_1 hk k_1^{-1} \text{ for all } h, h_1 \in H, k, k_1 \in K.$$

Use the orbit-stabiliser theorem to show that

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

Now we calculate the orbit of $1_G$. The orbit of the set, by definition, is

$$(H \times K).1_G = \{h_1 k_1^{-1} : h_1 \in H, k_1 \in K\},$$

which is simply $HK$.

# Orbit-stabiliser theorem

## Original example

Let $H$ and $K$ be two subgroups of the finite group $G$. $H \times K$ acts on $HK$ according to the map

$$(h_1, k_1).hk = h_1 hkk_1^{-1} \text{ for all } h, h_1 \in H, k, k_1 \in K.$$

Use the orbit-stabiliser theorem to show that

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

Putting all this together,

# Orbit-stabiliser theorem

## Original example

Let $H$ and $K$ be two subgroups of the finite group $G$. $H \times K$ acts on $HK$ according to the map

$$(h_1, k_1).hk = h_1 hk k_1^{-1} \text{ for all } h, h_1 \in H, k, k_1 \in K.$$

Use the orbit-stabiliser theorem to show that

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

Putting all this together, we have

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

# Orbit-stabiliser theorem

## Original example

Let $H$ and $K$ be two subgroups of the finite group $G$. $H \times K$ acts on $HK$ according to the map

$$(h_1, k_1).hk = h_1 hk k_1^{-1} \text{ for all } h, h_1 \in H, k, k_1 \in K.$$

Use the orbit-stabiliser theorem to show that

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

Putting all this together, we have

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

# Example of stabiliser (Centralisers)

## Definition (Centraliser)

The centraliser of $A \subseteq G$, written as $C_G(A)$, is the set of all elements of $G$ that fix the elements of $A$ under conjugation. That is,

$$C_G(A) = \{g \in G : ga = ag \text{ for all } a \in A\}.$$

It can be thought of as the intersection of the stabilisers of all elements in $A$ under conjugation.

Moreover, the centre of $G$, $Z(G)$, is $C_G(G)$, that is, the set of all elements that are completely fixed under conjugation.

## Example

For instance, what is the centre of $GL_n(\mathbb{C})$?

# Example of stabilisers (Centralisers)

**Theorem (The class equation)**

For $x_1, x_2, ..., x_t$ as representatives from the conjugacy classes of $G$ that have more than one element,

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)].$$

# Example of stabilisers (Centralisers)

**Theorem (The class equation)**

For $x_1, x_2, ..., x_t$ as representatives from the conjugacy classes of $G$ that have more than one element,

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)].$$

Remember that for all $g \in Z(G)$, $[G : C_G(g)] = 1$ since $C_G(g) = G$, so we can also write this formula as

$$|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$$

for $x_1, x_2, ..., x_n$ as representatives from all the conjugacy classes of $G$.

# Example of stabiliser (Centralisers)

## Original example

Let $G$ be a group of order $p^n$ where $p$ is prime. Show that the centre of $G$ is non-trivial.

# Example of stabiliser (Centralisers)

## Original example

Let $G$ be a group of order $p^n$ where $p$ is prime. Show that the centre of $G$ is non-trivial.

We are interested in the size of $Z(G)$. Consider the class equation

$$p^n = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)].$$

# Example of stabiliser (Centralisers)

## Original example

Let $G$ be a group of order $p^n$ where $p$ is prime. Show that the centre of $G$ is non-trivial.

We are interested in the size of $Z(G)$. Consider the class equation

$$p^n = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)].$$

Now $[G : C_G(x_i)]$ must divide $p^n$ but must not be trivial, since otherwise $x_i$ would lie in $Z(G)$.

# Example of stabiliser (Centralisers)

## Original example

Let $G$ be a group of order $p^n$ where $p$ is prime. Show that the centre of $G$ is non-trivial.

We are interested in the size of $Z(G)$. Consider the class equation

$$p^n = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)].$$

Now $[G : C_G(x_i)]$ must divide $p^n$ but must not be trivial, since otherwise $x_i$ would lie in $Z(G)$. So clearly $[G : C_G(x_i)]$ must divide $p$ for all $i = 1, 2, ..., n$. Hence, $|Z(G)|$ must divide $p$, meaning that $|Z(G)| \geq p \geq 2$. So the centre of $G$ is indeed non-trivial.

# Counting orbits

## Definition (Fixed point set)

Consider $H \subset G$ and $S$ a $G$-set. The fixed point set of $H$ is

$$S^H = \{s \in S : h.s = s \text{ for any } h \in H\}.$$

## Theorem (Counting orbits)

The number of orbits in the set $S$ is given by

$$|S/G| = \frac{1}{|G|} \sum_{g \in G} |S^g|.$$

# Counting orbits

**(2020, Question 2 iii)**

Let $G$ be a finite group acting transitively upon a finite set with more than one element. Show that there is an element $g \in G$ without fixed points.

If $G$ acts transitively on the set $S$, then $|S/G| = 1$.

# Counting orbits

**(2020, Question 2 iii)**

Let $G$ be a finite group acting transitively upon a finite set with more than one element. Show that there is an element $g \in G$ without fixed points.

If $G$ acts transitively on the set $S$, then $|S/G| = 1$. Hence,

$$1 = \frac{1}{|G|} \sum_{g \in G} |S^g|.$$

# Counting orbits

**(2020, Question 2 iii)**

Let $G$ be a finite group acting transitively upon a finite set with more than one element. Show that there is an element $g \in G$ without fixed points.

If $G$ acts transitively on the set $S$, then $|S/G| = 1$. Hence,

$$1 = \frac{1}{|G|} \sum_{g \in G} |S^g|.$$

Now our aim is to show that for at least one $g$, $|S^g| = 0$. Suppose that, instead, $|S^g| \geq 1$ for all $g$.

# Counting orbits

**(2020, Question 2 iii)**

Let $G$ be a finite group acting transitively upon a finite set with more than one element. Show that there is an element $g \in G$ without fixed points.

If $G$ acts transitively on the set $S$, then $|S/G| = 1$. Hence,

$$1 = \frac{1}{|G|} \sum_{g \in G} |S^g|.$$

Now our aim is to show that for at least one $g$, $|S^g| = 0$. Suppose that, instead, $|S^g| \geq 1$ for all $g$. But we know that for the identity element $1_G$, $|S^{1_G}| = \{s \in S : 1_G.s = s\} = |S| > 1$, since $S$ has more than one element. So it follows that

$$\sum_{g \in G} |S^g| > \underbrace{(1 + 1 + .... + 1)}_{|G| \text{ times}} = |G|$$

# Counting orbits

**(2020, Question 2 iii)**

Let $G$ be a finite group acting transitively upon a finite set with more than one element. Show that there is an element $g \in G$ without fixed points.

Hence,

$$\frac{1}{|G|} \sum_{g \in G} |S^g| > 1,$$

which is a contradiction. It follows that at least one element $g \in G$ must not have fixed points.

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. The elements of $D_4$ act on the square by rotations and reflections in the standard way. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

Let $S$ be the set of all distinct colourings of the edges of the square.

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. The elements of $D_4$ act on the square by rotations and reflections in the standard way. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

Let $S$ be the set of all distinct colourings of the edges of the square. We are not interested in $S$, but in the number of $D_4$-orbits of $S$, that is, the distinct colourings that cannot be obtained from applying $D_4$ to another of the colourings.

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. The elements of $D_4$ act on the square by rotations and reflections in the standard way. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

Let $S$ be the set of all distinct colourings of the edges of the square. We are not interested in $S$, but in the number of $D_4$-orbits of $S$, that is, the distinct colourings that cannot be obtained from applying $D_4$ to another of the colourings. So

$$|S/D_4| = \frac{1}{8}\sum_{g\in G} |S^g|.$$

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

Now we break down the fixed point sets of each of the 8 elements $g \in G$. First of all,

$$|S^{\mathrm{id}}| = |S| = n^4.$$

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

Now we break down the fixed point sets of each of the 8 elements $g \in G$. First of all,

$$|S^{\mathrm{id}}| = |S| = n^4.$$

There are two $90°$ rotations that turn the edges into a 4-cycle, so in these cases

$$|S^g| = n$$

since then we have $n$ options for what to colour the 4-cycle.

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

We have one remaining rotation, which is a 180° rotation. This rotation creates two 2-cycles, meaning that

$$|S^g| = n^2$$

since then we have $n$ options for what to colour each of the 2-cycles.

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

Finally, we have our reflections.

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

Finally, we have our reflections. Two of the reflections are reflections about diagonals, which generate two 2-cycles, and hence

$$|S^g| = n^2.$$

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

Finally, we have our reflections. Two of the reflections are reflections about diagonals, which generate two 2-cycles, and hence

$$|S^g| = n^2.$$

The remaining two reflections are reflections about axes joining the midpoints of opposite edges, which fix two edges and generate one 2-cycle. In these cases, then,

$$|S^g| = n^3.$$

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

So in summary,

# Counting orbits

**(2017, Question 1 d)**

Consider a square in $\mathbb{R}^2$ centred at the origin. Find the number of colourings of the edges of the square in $n$ colours, where two colourings are considered equivalent if one can be obtained from the other by applying an element of $D_4$. Your answer should be given as a polynomial in $n$.

So in summary,

$$\begin{aligned} |S/G| &= \frac{1}{8}(n^4 + 2n^3 + 2n^2 + n^2 + 2n) \\ &= \frac{1}{8}(n^4 + 2n^3 + 3n^2 + 2n). \end{aligned}$$

# 5. Rings

# Rings

We will now look at specific kinds of algebraic structures

# Rings

We will now look at specific kinds of algebraic structures – additive groups which have a second operation: multiplication.

# Rings

We will now look at specific kinds of algebraic structures – additive groups which have a second operation: multiplication.
A ring is a set $R$ equipped with an additive $(+)$ and a multiplicative $(\times)$ operation that satisfy the following properties:

# Rings

We will now look at specific kinds of algebraic structures – additive groups which have a second operation: multiplication.
A ring is a set $R$ equipped with an additive $(+)$ and a multiplicative $(\times)$ operation that satisfy the following properties:

**Addition**

$R$ is an **abelian group**.

$R$ is closed.
$R$ is associative.
$R$ is commutative.
$R$ has the additive identity element.
Every element in $R$ has an additive inverse.

# Rings

We will now look at specific kinds of algebraic structures – additive groups which have a second operation: multiplication.
A ring is a set $R$ equipped with an additive $(+)$ and a multiplicative $(\times)$ operation that satisfy the following properties:

**Addition**

$R$ is an **abelian group**.

$R$ is closed.
$R$ is associative.
$R$ is commutative.
$R$ has the additive identity element.
Every element in $R$ has an additive inverse.

**Multiplication**

$R$ is closed.

$R$ is associative.

# Rings

We will now look at specific kinds of algebraic structures – additive groups which have a second operation: multiplication.
A ring is a set $R$ equipped with an additive $(+)$ and a multiplicative $(\times)$ operation that satisfy the following properties:

**Addition**

$R$ is an **abelian group**.

$R$ is closed.
$R$ is associative.
$R$ is commutative.
$R$ has the additive identity element.
Every element in $R$ has an additive inverse.

**Multiplication**

$R$ is closed.

$R$ is associative.

The operations satisfy the distribution properties

$$(a+b)\times c = a\times c + b\times c, \quad a\times(b+c) = a\times b + a\times c$$

for all $a, b, c \in R$

# Ideals and quotient rings – motivation

Consider an additive subgroup $I$ of a ring, $R$. What sort of properties should we impose on $I$ so that $R/I$ forms a ring?

# Ideals and quotient rings – motivation

Consider an additive subgroup $I$ of a ring, $R$. What sort of properties should we impose on $I$ so that $R/I$ forms a ring?

The **cosets** come in the form $R/I = r + I = \{r + i \mid i \in I\}$ for all $r \in R$.

# Ideals and quotient rings – motivation

Consider an additive subgroup $I$ of a ring, $R$. What sort of properties should we impose on $I$ so that $R/I$ forms a ring?

The **cosets** come in the form $R/I = r + I = \{r + i \mid i \in I\}$ for all $r \in R$.

Multiplication makes sense when

$$(a + i)(b + i') = ab + I,$$

for all $a, b \in R$ and $i, i' \in I$. We have that

$$(a + i)(b + i') = ab + ai' + ib + ii' \equiv ab + I \implies ai' \in I, ib \in I.$$

# Ideals and quotient rings – motivation

Consider an additive subgroup $I$ of a ring, $R$. What sort of properties should we impose on $I$ so that $R/I$ forms a ring?

The **cosets** come in the form $R/I = r + I = \{r + i \mid i \in I\}$ for all $r \in R$.

Multiplication makes sense when

$$(a + i)(b + i') = ab + I,$$

for all $a, b \in R$ and $i, i' \in I$. We have that

$$(a + i)(b + i') = ab + ai' + ib + ii' \equiv ab + I \implies ai' \in I, ib \in I.$$

This motivates our definition for an *ideal*.

# Ideals and quotient rings – definition

Let $R$ be a ring.

# Ideals and quotient rings – definition

Let $R$ be a ring.

## Ideal

Let $I$ be a subgroup of $R$. Then $I$ is an ideal if:

$(I, +)$ is a group.

For all $r \in R$ and $x \in I$, $rx \in I$ and $xr \in I$.

# Ideals and quotient rings – definition

Let $R$ be a ring.

**Ideal**

Let $I$ be a subgroup of $R$. Then $I$ is an ideal if:

$(I, +)$ is a group.

For all $r \in R$ and $x \in I$, $rx \in I$ and $xr \in I$.

We denote an ideal analogously to normal subgroups; that is, $I \trianglelefteq R$. In fact, ideals operate really closely to normal subgroups!

# Ideals and quotient rings – definition

Let $R$ be a ring.

## Ideal

Let $I$ be a subgroup of $R$. Then $I$ is an ideal if:

$(I, +)$ is a group.

For all $r \in R$ and $x \in I$, $rx \in I$ and $xr \in I$.

We denote an ideal analogously to normal subgroups; that is, $I \trianglelefteq R$. In fact, ideals operate really closely to normal subgroups!

## Note

Since 1 need not be in $R$, $I$ may not be a subring. In fact, if $1 \in I$, then $I$ is identically $R$.

## (2019, Q2 a)

Let $I$ and $J$ be ideals of a ring $R$. Prove that $I + J = \{x + y \mid x \in I, y \in J\}$ is an ideal. Is $K = \{xy \mid x \in I, y \in J\}$ an ideal in $R$?

## (2019, Q2 a)

Let $I$ and $J$ be ideals of a ring $R$. Prove that $I + J = \{x + y \mid x \in I, y \in J\}$ is an ideal. Is $K = \{xy \mid x \in I, y \in J\}$ an ideal in $R$?

Since $I, J \leq R$, it also follows that $I + J \leq R$ and $(I + J, +)$ forms an abelian group.

## (2019, Q2 a)

Let $I$ and $J$ be ideals of a ring $R$. Prove that $I + J = \{x + y \mid x \in I, y \in J\}$ is an ideal. Is $K = \{xy \mid x \in I, y \in J\}$ an ideal in $R$?

Since $I, J \leq R$, it also follows that $I + J \leq R$ and $(I + J, +)$ forms an abelian group. Now take $a \in R$ and $x \in I, y \in J$ so that $x + y \in I + J$. Then we have that

$$a(x + y) = \underbrace{ax}_{\in I} + \underbrace{ay}_{\in J} \in I + J.$$

A similar argument can be made for the right ideal.

## (2019, Q2 a)

Let $I$ and $J$ be ideals of a ring $R$. Prove that $I + J = \{x + y \mid x \in I, y \in J\}$ is an ideal. Is $K = \{xy \mid x \in I, y \in J\}$ an ideal in $R$?

We now show that $K$ is *not* an ideal.

## (2019, Q2 a)

Let $I$ and $J$ be ideals of a ring $R$. Prove that $I + J = \{x + y \mid x \in I, y \in J\}$ is an ideal. Is $K = \{xy \mid x \in I, y \in J\}$ an ideal in $R$?

We now show that $K$ is *not* an ideal.
Consider the ring $\mathbb{Z}[x]$ and consider the ideals $I = (2, x)$ and $J = (5, x)$.

## (2019, Q2 a)

Let $I$ and $J$ be ideals of a ring $R$. Prove that $I + J = \{x + y \mid x \in I, y \in J\}$ is an ideal. Is $K = \{xy \mid x \in I, y \in J\}$ an ideal in $R$?

We now show that $K$ is *not* an ideal.
Consider the ring $\mathbb{Z}[x]$ and consider the ideals $I = (2, x)$ and $J = (5, x)$.
We claim that $K$, under these ideals, does not form an ideal.

## (2019, Q2 a)

Let $I$ and $J$ be ideals of a ring $R$. Prove that $I + J = \{x + y \mid x \in I, y \in J\}$ is an ideal. Is $K = \{xy \mid x \in I, y \in J\}$ an ideal in $R$?

We now show that $K$ is *not* an ideal.
Consider the ring $\mathbb{Z}[x]$ and consider the ideals $I = (2, x)$ and $J = (5, x)$. We claim that $K$, under these ideals, does not form an ideal. We observe that $x \notin K$.

## (2019, Q2 a)

Let $I$ and $J$ be ideals of a ring $R$. Prove that $I + J = \{x + y \mid x \in I, y \in J\}$ is an ideal. Is $K = \{xy \mid x \in I, y \in J\}$ an ideal in $R$?

We now show that $K$ is *not* an ideal.
Consider the ring $\mathbb{Z}[x]$ and consider the ideals $I = (2, x)$ and $J = (5, x)$. We claim that $K$, under these ideals, does not form an ideal. We observe that $x \notin K$. But, if $K$ were to be an ideal, then $5x - 2 \cdot 2x = x \in K$ which is a contradiction. Hence, $K$ is not an ideal.

## (2021, Q2 iv)

If $R$ is a commutative ring, let $I = \{x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N}\}$. Prove that $I$ is an ideal.

**(2021, Q2 iv)**

If $R$ is a commutative ring, let $I = \{x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N}\}$. Prove that $I$ is an ideal.

*Part I*: Show that $(I, +)$ is an abelian group.

## (2021, Q2 iv)

If $R$ is a commutative ring, let $I = \{x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N}\}$. Prove that $I$ is an ideal.

*Part I*: Show that $(I, +)$ is an abelian group.
Associativity and commutativity follows from $R$. Let $x, y \in I$. Then $x^n = 0$ and $y^m = 0$. It follows that $(x + y)^{n+m} = 0$. Hence, $I$ is closed. $0^1 = 0$ and if $x^n = 0$, then $(-x)^n = 0$. So $(I, +)$ is an abelian group.

## (2021, Q2 iv)

If $R$ is a commutative ring, let $I = \{x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N}\}$. Prove that $I$ is an ideal.

*Part II*: If $r \in R$ and $x \in I$, then $rx \in I$ and $xr \in I$.

## (2021, Q2 iv)

If $R$ is a commutative ring, let $I = \{x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N}\}$. Prove that $I$ is an ideal.

*Part II*: If $r \in R$ and $x \in I$, then $rx \in I$ and $xr \in I$.
We have

$$\begin{aligned}(rx)^n &= (rx)(rx)\dots(rx) \\ &= r^n x^n && (R \text{ is a commutative ring}) \\ &= 0. && (x \in I)\end{aligned}$$

Hence, $rx \in I$. It follows that $xr \in I$. Hence, $I$ is an ideal.

# Ideals – properties

Let $I_1, I_2, \ldots, I_n$ be ideals of a ring $R$. Then $I = \bigcap_j I_j$ is an ideal of $R$.

# Ideals – properties

Let $I_1, I_2, \ldots, I_n$ be ideals of a ring $R$. Then $I = \bigcap_j I_j$ is an ideal of $R$.

If $R$ is a field, then there are precisely two ideals: $\{0\}$ and $R$.

# Ideals – properties

Let $I_1, I_2, \ldots, I_n$ be ideals of a ring $R$. Then $I = \bigcap_j I_j$ is an ideal of $R$.

If $R$ is a field, then there are precisely two ideals: $\{0\}$ and $R$.

Let $S \subseteq R$. The ideal generated by $S$ is $\langle S \rangle := \bigcap_{I \in \Lambda} I$ where $\Lambda$ is the set of all ideals that contains $S$.

# Ideals – principal ideals

Let $I$ be an ideal of $R$. If $I$ is finitely generated, then we can express $I$ using the basis elements: $I = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. We call $I$ a *principal ideal* if it can be generated by one element; that is, for some $\alpha \in R$, $I = (\alpha)$.

# Ideals – principal ideals

Let $I$ be an ideal of $R$. If $I$ is finitely generated, then we can express $I$ using the basis elements: $I = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. We call $I$ a *principal ideal* if it can be generated by one element; that is, for some $\alpha \in R$, $I = (\alpha)$.

**(2021, Q2 iii)**

Show that the ideal $(3, x^3 - x^2 + 2x - 1)$ in $\mathbb{Z}[x]$ is not principal.

## (2021, Q2 iii)

Show that the ideal $(3, x^3 - x^2 + 2x - 1)$ in $\mathbb{Z}[x]$ is not principal.

Suppose that there exist some $\alpha \in \mathbb{Z}[x]$ such that $(\alpha) = (3, x^3 - x^2 + 2x - 1)$.

## (2021, Q2 iii)

Show that the ideal $(3, x^3 - x^2 + 2x - 1)$ in $\mathbb{Z}[x]$ is not principal.

Suppose that there exist some $\alpha \in \mathbb{Z}[x]$ such that $(\alpha) = (3, x^3 - x^2 + 2x - 1)$. Then $\alpha$ generates 3 and $x^3 - x^2 + 2x - 1$. So $\alpha \mid 3$ and $\alpha \mid x^3 - x^2 + 2x - 1$.

## (2021, Q2 iii)

Show that the ideal $(3, x^3 - x^2 + 2x - 1)$ in $\mathbb{Z}[x]$ is not principal.

Suppose that there exist some $\alpha \in \mathbb{Z}[x]$ such that $(\alpha) = (3, x^3 - x^2 + 2x - 1)$. Then $\alpha$ generates 3 and $x^3 - x^2 + 2x - 1$. So $\alpha \mid 3$ and $\alpha \mid x^3 - x^2 + 2x - 1$.
$\alpha \mid 3$ implies that $\alpha \in \{\pm 1, \pm 3\}$. We see that, if $\alpha \in \{-3, 3\}$, then $\alpha \nmid x^3 - x^2 + 2x - 1$. So $\alpha \in \{-1, 1\}$ but then $(\alpha)$ is the entire ring. This is impossible because $x \notin (3, x^3 - x^2 + 2x - 1)$. Hence, the ideal cannot be principal.

# Ideals – maximal ideals

Let $I$ be an ideal of $R$. We say that $I$ is maximal if we can't fit another ideal between $I$ and $R$.

# Ideals – maximal ideals

Let $I$ be an ideal of $R$. We say that $I$ is maximal if we can't fit another ideal between $I$ and $R$.

## Maximal ideal

An ideal $I \trianglelefteq R$, with $I \neq R$, is *maximal* if it is maximal amongst ideals not equal to $R$. That is, if $J \trianglelefteq R$ and $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

# Ideals – maximal ideals

Let $I$ be an ideal of $R$. We say that $I$ is maximal if we can't fit another ideal between $I$ and $R$.

**Maximal ideal**

An ideal $I \trianglelefteq R$, with $I \neq R$, is *maximal* if it is maximal amongst ideals not equal to $R$. That is, if $J \trianglelefteq R$ and $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

**(Result)**

It turns out that if we consider the quotient ring with a maximal ideal, then the quotient ring actually forms a field. That is, if $I \trianglelefteq R$ and $I$ is maximal, then $R/I$ is precisely a field.

# Ideals – prime ideals

Let $R$ be a commutative ring. Let $I \trianglelefteq R$ with $I \neq R$. We say that $I$ is a *prime ideal* if $rs \in I$ implies that $r \in I$ or $s \in I$.

**(Result)**

Every *maximal* ideal is a prime ideal. The converse is not necessarily true.

## (Problem Set 10, Q4)

Show that $I = (2, 1 + \sqrt{-5})$ is a prime ideal of $\mathbb{Z}[\sqrt{-5}]$.

## (Problem Set 10, Q4)

Show that $I = (2, 1 + \sqrt{-5})$ is a prime ideal of $\mathbb{Z}[\sqrt{-5}]$.

We will actually prove that the ideal $I$ is maximal; $I$ being prime is a consequence.
If we want to show that $I$ is maximal, it suffices to prove that $\mathbb{Z}[\sqrt{-5}]/I$ is a field. We now write the quotient ring until we can see a field pop up:

$$\begin{aligned} \mathbb{Z}[\sqrt{-5}] &\cong \mathbb{Z}[X]/(X^2 + 5) \\ \mathbb{Z}[\sqrt{-5}]/(2, 1 + \sqrt{-5}) &\cong \mathbb{Z}[X]/(2, X^2 + 5, 1 + X) \\ &\cong \mathbb{F}_2[X]/(X^2 + 5, 1 + X) \\ &\cong \mathbb{F}_2[X]. \end{aligned}$$

Hence, $(2, 1 + \sqrt{-5})$ is a maximal ideal which also implies that the ideal is prime.

# Chinese Remainder Theorem for rings

We begin with the statement of the Chinese Remainder Theorem on integers before generalising it to arbitrary rings.

# Chinese Remainder Theorem for rings

We begin with the statement of the Chinese Remainder Theorem on integers before generalising it to arbitrary rings.

Let $n_1, n_2, \ldots, n_k \in \mathbb{Z}^+$ such that $n_i$ and $n_j$ are coprime pairs for each $i \neq j$. Then, for any $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, there exist a unique solution modulo $n = n_1 n_2 \ldots n_k$ to the simultaneous equations

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\ldots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

# Chinese Remainder Theorem for rings

We begin with the statement of the Chinese Remainder Theorem on integers before generalising it to arbitrary rings.

Let $n_1, n_2, \ldots, n_k \in \mathbb{Z}^+$ such that $n_i$ and $n_j$ are coprime pairs for each $i \neq j$. Then, for any $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, there exist a unique solution modulo $n = n_1 n_2 \ldots n_k$ to the simultaneous equations

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\ldots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

We now generalise this statement to arbitrary rings.

# Chinese Remainder Theorem for rings

Let $R$ be a ring and $I_1, I_2, \ldots, I_k$ be ideals of $R$. Suppose that $I_i + I_j = R$ for each pair and $i \neq j$. Let $I = \bigcap_j I_j$, which is also an ideal. Then we have the isomorphism:

$$\phi : R/I \to R/I_1 \times R/I_2 \times \ldots R/I_k, \quad r + I \mapsto (r + I_1, r + I_2, \ldots, r + I_k).$$

# Chinese Remainder Theorem for rings

Let $R$ be a ring and $I_1, I_2, \ldots, I_k$ be ideals of $R$. Suppose that $I_i + I_j = R$ for each pair and $i \neq j$. Let $I = \bigcap_j I_j$, which is also an ideal. Then we have the isomorphism:

$$\phi : R/I \to R/I_1 \times R/I_2 \times \ldots R/I_k, \quad r + I \mapsto (r + I_1, r + I_2, \ldots, r + I_k).$$

Another way of looking at $I_i + I_j = R$ is to say that there exist some $i \in I_i$ and $j \in I_j$ such that $i + j = 1$.

# Chinese Remainder Theorem for rings

Let $R$ be a ring and $I_1, I_2, \ldots, I_k$ be ideals of $R$. Suppose that $I_i + I_j = R$ for each pair and $i \neq j$. Let $I = \bigcap_j I_j$, which is also an ideal. Then we have the isomorphism:

$$\phi : R/I \to R/I_1 \times R/I_2 \times \ldots R/I_k, \quad r + I \mapsto (r + I_1, r + I_2, \ldots, r + I_k).$$

Another way of looking at $I_i + I_j = R$ is to say that there exist some $i \in I_i$ and $j \in I_j$ such that $i + j = 1$. Then the element 1 belongs in the ideal $I_i + I_j$ and so it generates all of $R$.

## (2020, Q4 ii)

Let $M_1 \neq M_2$ be two maximal ideals in the commutative ring and $I = M_1 \cap M_2$. Prove that $R/I$ is isomorphic to a direct sum of two fields.

## (2020, Q4 ii)

Let $M_1 \neq M_2$ be two maximal ideals in the commutative ring and $I = M_1 \cap M_2$. Prove that $R/I$ is isomorphic to a direct sum of two fields.

Recall that:

If $I$ is a maximal ideal of a ring $R$, then $R/I$ is field.

## (2020, Q4 ii)

Let $M_1 \neq M_2$ be two maximal ideals in the commutative ring and $I = M_1 \cap M_2$. Prove that $R/I$ is isomorphic to a direct sum of two fields.

Recall that:

> If $I$ is a maximal ideal of a ring $R$, then $R/I$ is field.

Note that $M_1 \subsetneq M_1 + M_2 \subseteq R$ and similarly, $M_2 \subsetneq M_1 + M_2 \subseteq R$ because $M_1 \neq M_2$.

## (2020, Q4 ii)

Let $M_1 \neq M_2$ be two maximal ideals in the commutative ring and $I = M_1 \cap M_2$. Prove that $R/I$ is isomorphic to a direct sum of two fields.

Recall that:

> If $I$ is a maximal ideal of a ring $R$, then $R/I$ is field.

Note that $M_1 \subsetneq M_1 + M_2 \subseteq R$ and similarly, $M_2 \subsetneq M_1 + M_2 \subseteq R$ because $M_1 \neq M_2$. This implies that $M_1 + M_2 = R$ since $M_1$ and $M_2$ are maximal.

## (2020, Q4 ii)

Let $M_1 \neq M_2$ be two maximal ideals in the commutative ring and $I = M_1 \cap M_2$. Prove that $R/I$ is isomorphic to a direct sum of two fields.

Recall that:

> If $I$ is a maximal ideal of a ring $R$, then $R/I$ is field.

Note that $M_1 \subsetneq M_1 + M_2 \subseteq R$ and similarly, $M_2 \subsetneq M_1 + M_2 \subseteq R$ because $M_1 \neq M_2$. This implies that $M_1 + M_2 = R$ since $M_1$ and $M_2$ are maximal. By the Chinese Remainder Theorem, we obtain the isomorphism

$$R/(M_1 \cap M_2) \cong R/M_1 \oplus R/M_2,$$

which is a direct sum of two fields.

# Integral domains

## Integral domain

A *commutative ring* $R$ is said to be an *integral domain* if $rs = 0$ implies that $r = 0$ or $s = 0$ for all $r, s \in R$.

# Integral domains

## Integral domain

A *commutative ring* $R$ is said to be an *integral domain* if $rs = 0$ implies that $r = 0$ or $s = 0$ for all $r, s \in R$.

This is convenient because the usual *cancellation law* applies to domains but not on rings in general. That is, if $u \neq 0$ and $uv = uw$, then $v = w$ because $uv - uw = 0$ implies that $u(v - w) = 0$ which implies that $v = w$.

# Integral domains

## Integral domain

A *commutative ring* $R$ is said to be an *integral domain* if $rs = 0$ implies that $r = 0$ or $s = 0$ for all $r, s \in R$.

This is convenient because the usual *cancellation law* applies to domains but not on rings in general. That is, if $u \neq 0$ and $uv = uw$, then $v = w$ because $uv - uw = 0$ implies that $u(v - w) = 0$ which implies that $v = w$.

## (Result)

It turns out that if we consider the quotient ring with a *prime* ideal, then quotient ring forms an integral domain. That is, if $I$ is a prime ideal, then $R/I$ forms an integral domain.

# Integral domains

**(2021, Q2 i)**

Is $\mathbb{Z} \oplus \mathbb{Z}$ an integral domain? Justify your answer.

# Integral domains

**(2021, Q2 i)**

Is $\mathbb{Z} \oplus \mathbb{Z}$ an integral domain? Justify your answer.

Recall that an integral domain requires $rs = 0$ implying that $r = 0$ or $s = 0$.

# Integral domains

**(2021, Q2 i)**

Is $\mathbb{Z} \oplus \mathbb{Z}$ an integral domain? Justify your answer.

Recall that an integral domain requires $rs = 0$ implying that $r = 0$ or $s = 0$.

Take $(1, 0)$ and $(0, 1)$, both of which belong in $\mathbb{Z} \oplus \mathbb{Z}$. But we see that $(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$. Hence, $\mathbb{Z} \oplus \mathbb{Z}$ is not an integral domain.

# Fraction Fields – motivation

Every field is an integral domain but the converse isn't necessarily true. For example, $\mathbb{Z}$ forms an integral domain but not a field. One thing we can ask is: *given an integral domain $D$, how might we like to associate it with a field?*

Let $D$ be an integral domain and suppose that

$$S = \{(a, b) : a, b \in D \text{ with } b \neq 0\}.$$

The relation $(a, b) \sim (c, d)$ if $ad = bc$ is an equivalence relation.

# Fraction Fields – motivation

Every field is an integral domain but the converse isn't necessarily true. For example, $\mathbb{Z}$ forms an integral domain but not a field. One thing we can ask is: *given an integral domain $D$, how might we like to associate it with a field?*

Let $D$ be an integral domain and suppose that

$$S = \{(a, b) : a, b \in D \text{ with } b \neq 0\}.$$

The relation $(a, b) \sim (c, d)$ if $ad = bc$ is an equivalence relation.

The usual addition and multiplication operations on the equivalence classes formed by the equivalence relation are well defined. It turns out that this actually forms a field!

# Fraction Fields – motivation

Every field is an integral domain but the converse isn't necessarily true. For example, $\mathbb{Z}$ forms an integral domain but not a field. One thing we can ask is: *given an integral domain $D$, how might we like to associate it with a field?*

Let $D$ be an integral domain and suppose that

$$S = \{(a, b) : a, b \in D \text{ with } b \neq 0\}.$$

The relation $(a, b) \sim (c, d)$ if $ad = bc$ is an equivalence relation.

The usual addition and multiplication operations on the equivalence classes formed by the equivalence relation are well defined. It turns out that this actually forms a field!
We call this the *fraction field* of $D$. We denote the fraction field of $D$ as $K(D)$. We will talk about fields more explicitly later!

# Fraction Fields

If $F$ is a field, then $K(F) = F$.

If $S$ is a subring of $R$, then $K(S)$ is a subring of $K(R)$.

If $R$ is a subfield of $F$, then $K(R)$ is a subfield of $K(F) = F$.

# Unique Factorisation Domains I

In $\mathbb{Z}$, we see that any integer can be written as a (unique) product of primes up to reordering. But the same cannot be said for an arbitrary ring. For example, $\mathbb{Z}[\sqrt{-5}]$ factors 6 into $3 \times 2$ or $(1+\sqrt{-5})(1-\sqrt{-5})$. Each of these elements are *prime* so we no longer have unique factorisation.
We will now develop theory to define a domain in which we have unique factorisation.

# Unique Factorisation Domains II

Consider a commutative domain $R$ and let $r, s \in R$.

- We say that $r$ is a **factor** of $s$, or that $r$ divides $s$, if there exist some $t \in R$ such that $s = rt$.
- We say that $r$ and $s$ are **associates** if there exist a unit $u \in R^*$ such that $r = su$.
- We say that a non-zero and non-unit element $r$ is **irreducible** if every factor of $r$ is either a unit or an associate of $r$.
- We say that a non-zero and non-unit element $p$ is **prime** if $p \mid rs$ implies that $p \mid r$ or $p \mid s$ for all $r, s \in R$.

# Unique Factorisation Domains II

Consider a commutative domain $R$ and let $r, s \in R$.

- We say that $r$ is a **factor** of $s$, or that $r$ divides $s$, if there exist some $t \in R$ such that $s = rt$.
- We say that $r$ and $s$ are **associates** if there exist a unit $u \in R^*$ such that $r = su$.
- We say that a non-zero and non-unit element $r$ is **irreducible** if every factor of $r$ is either a unit or an associate of $r$.
- We say that a non-zero and non-unit element $p$ is **prime** if $p \mid rs$ implies that $p \mid r$ or $p \mid s$ for all $r, s \in R$.

We now set up a parallel between principal ideals and factorisation.

# Unique Factorisation Domains III

- $r \mid s$ if and only if $\langle s \rangle \subseteq \langle r \rangle$.
- $r$ and $s$ are associates if and only if $\langle r \rangle = \langle s \rangle$.
- A non-zero and non-unit element $p$ is irreducible if and only if the only principal ideals that contain $\langle p \rangle$ are $\langle p \rangle$ and $\langle 1 \rangle$.
- A non-zero and non-unit element $p$ is prime if and only if $\langle p \rangle$ is a prime ideal.

In a commutative domain, every prime element is irreducible. The converse, however, is not necessarily true; that is, irreducible elements are not necessarily prime.

# Unique Factorisation Domains IV

## Unique Factorisation Domains (UFDs)

Let $R$ be a commutative domain. We say that $R$ is a *unique factorisation domain* if the following hold:

- For any non-zero and non-unit element $r \in R$, we have that

$$r = p_1 p_2 \dots p_m$$

  where $p_i$ is irreducible for $1 \leq i \leq m$.
- If we have two factorisations of the same element $r = p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$, then $m = n$ and we can re-index $q_i$ so that $q_i$ and $p_i$ are associates for all $i$.

## Factorisation over $\mathbb{Z}$

We see that $10 = 5 \times 2$ but we can also factor 10 as $10 = -5 \times -2$. $-5$ and 5 are associates, and 2 and $-2$ are associates.

# Unique Factorisation Domains V

## Unique Factorisation Domains (UFDs)

Let $R$ be a commutative domain. We say that $R$ is a *unique factorisation domain* if the following hold:

- For any non-zero and non-unit element $r \in R$, we have that

$$r = p_1 p_2 \dots p_m$$

  where $p_i$ is irreducible for $1 \leq i \leq m$.
- If we have two factorisations of the same element $r = p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$, then $m = n$ and we can re-index $q_i$ so that $q_i$ and $p_i$ are associates for all $i$.

We can relax the second condition. It turns out that, if every irreducible element is prime, then it is enough for $R$ to be a UFD!

## (Problem Set 10, Q1)

Show that, if $R$ is a UFD, then any two nonzero elements have a gcd.

## (Problem Set 10, Q1)

Show that, if $R$ is a UFD, then any two nonzero elements have a gcd.

Any element in $R$ can be decomposed into a product of irreducible elements (i.e. prime elements). Thus, we can write

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}, \quad b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k},$$

where each $p_i$ is a prime element. Then we have that

$$\gcd(a, b) = \prod_{i=1}^{k} p_i^{\min(n_i, m_i)}$$

which is well-defined.

## (2021, Q3 i)

Show that 21 doesn't factor uniquely as a product of irreducibles in $\mathbb{Z}[\sqrt{-5}]$.

**(2021, Q3 i)**

Show that 21 doesn't factor uniquely as a product of irreducibles in $\mathbb{Z}[\sqrt{-5}]$.

Note that $21 = 7 \times 3 = (4 + \sqrt{-5})(4 - \sqrt{-5})$. It turns out that these elements are irreducible! This shows that 21 doesn't factor uniquely.

# Principal Ideal Domains I

Recall that a principal ideal is an ideal that is generated by a single element. We've also given some parallel definitions of factorisation with principal ideals.

- $r \mid s$ if and only if $\langle s \rangle \subseteq \langle r \rangle$.
- $r$ and $s$ are associates if and only if $\langle r \rangle = \langle s \rangle$.
- A non-zero and non-unit element $p$ is irreducible if and only if the only principal ideals that contain $\langle p \rangle$ are $\langle p \rangle$ and $\langle 1 \rangle$.
- A non-zero and non-unit element $p$ is prime if and only if $\langle p \rangle$ is a prime ideal.

We now define a principal ideal domain (PID).

# Principal Ideal Domains I

Recall that a principal ideal is an ideal that is generated by a single element. We've also given some parallel definitions of factorisation with principal ideals.

- $r \mid s$ if and only if $\langle s \rangle \subseteq \langle r \rangle$.
- $r$ and $s$ are associates if and only if $\langle r \rangle = \langle s \rangle$.
- A non-zero and non-unit element $p$ is irreducible if and only if the only principal ideals that contain $\langle p \rangle$ are $\langle p \rangle$ and $\langle 1 \rangle$.
- A non-zero and non-unit element $p$ is prime if and only if $\langle p \rangle$ is a prime ideal.

We now define a principal ideal domain (PID).

## Principal Ideal Domains (PIDs)

Let $R$ be a commutative domain. $R$ is a principal ideal domain if every ideal is principal.

# Principal Ideal Domains II

Let $R$ be a PID. Then every irreducible element in $R$ is prime.

# Principal Ideal Domains II

Let $R$ be a PID. Then every irreducible element in $R$ is prime.

Consider some irreducible element $p \in R \setminus \{0\}$. Consider the ideal generated by $p$. Since $p$ is irreducible, then the only principal ideals that contain $\langle p \rangle$ are $\langle p \rangle$ and $\langle 1 \rangle$. This implies that $\langle p \rangle$ is maximal and hence, is prime.

# Principal Ideal Domains II

Let $R$ be a PID. Then every irreducible element in $R$ is prime.

Consider some irreducible element $p \in R \setminus \{0\}$. Consider the ideal generated by $p$. Since $p$ is irreducible, then the only principal ideals that contain $\langle p \rangle$ are $\langle p \rangle$ and $\langle 1 \rangle$. This implies that $\langle p \rangle$ is maximal and hence, is prime.

Let $R$ be a PID. Then every non-zero and non-unit element $r \in R$ can be factored into a product of irreducible elements.

# Principal Ideal Domains II

Let $R$ be a PID. Then every irreducible element in $R$ is prime.

Consider some irreducible element $p \in R \setminus \{0\}$. Consider the ideal generated by $p$. Since $p$ is irreducible, then the only principal ideals that contain $\langle p \rangle$ are $\langle p \rangle$ and $\langle 1 \rangle$. This implies that $\langle p \rangle$ is maximal and hence, is prime.

Let $R$ be a PID. Then every non-zero and non-unit element $r \in R$ can be factored into a product of irreducible elements.

From the previous two results above, it turns out that PIDs are UFDs!

# Principal Ideal Domains II

Let $R$ be a PID. Then every irreducible element in $R$ is prime.

Consider some irreducible element $p \in R \setminus \{0\}$. Consider the ideal generated by $p$. Since $p$ is irreducible, then the only principal ideals that contain $\langle p \rangle$ are $\langle p \rangle$ and $\langle 1 \rangle$. This implies that $\langle p \rangle$ is maximal and hence, is prime.

Let $R$ be a PID. Then every non-zero and non-unit element $r \in R$ can be factored into a product of irreducible elements.

From the previous two results above, it turns out that PIDs are UFDs!

So we have

$$\text{ED} \subseteq \text{PID} \subseteq \text{UFD}$$

## (Problem Set 10, Q5)

Show that $\mathbb{Z}[x]$ is not a PID.

## (Problem Set 10, Q5)

Show that $\mathbb{Z}[x]$ is not a PID.

If $\mathbb{Z}[x]$ were to be a PID, then every ideal is principal.

## (Problem Set 10, Q5)

Show that $\mathbb{Z}[x]$ is not a PID.

If $\mathbb{Z}[x]$ were to be a PID, then every ideal is principal. Consider the ideal $I = \langle 2, x \rangle$. Suppose that $I$ was principal.

## (Problem Set 10, Q5)

Show that $\mathbb{Z}[x]$ is not a PID.

If $\mathbb{Z}[x]$ were to be a PID, then every ideal is principal. Consider the ideal $I = \langle 2, x \rangle$. Suppose that $I$ was principal. Then there exist some $\alpha \in \mathbb{Z}[x]$ such that

$$\langle \alpha \rangle = \langle 2, x \rangle.$$

## (Problem Set 10, Q5)

Show that $\mathbb{Z}[x]$ is not a PID.

If $\mathbb{Z}[x]$ were to be a PID, then every ideal is principal. Consider the ideal $I = \langle 2, x \rangle$. Suppose that $I$ was principal. Then there exist some $\alpha \in \mathbb{Z}[x]$ such that

$$\langle \alpha \rangle = \langle 2, x \rangle.$$

But then this implies that $\alpha \mid 2$ and $\alpha \mid x$. If $\alpha \mid 2$, then $\alpha \in \{\pm 1, \pm 2\}$. If $\alpha \in \{-2, 2\}$, then $\alpha \nmid x$.

## (Problem Set 10, Q5)

Show that $\mathbb{Z}[x]$ is not a PID.

If $\mathbb{Z}[x]$ were to be a PID, then every ideal is principal. Consider the ideal $I = \langle 2, x \rangle$. Suppose that $I$ was principal. Then there exist some $\alpha \in \mathbb{Z}[x]$ such that

$$\langle \alpha \rangle = \langle 2, x \rangle.$$

But then this implies that $\alpha \mid 2$ and $\alpha \mid x$. If $\alpha \mid 2$, then $\alpha \in \{\pm 1, \pm 2\}$. If $\alpha \in \{-2, 2\}$, then $\alpha \nmid x$. Hence, $\alpha \in \{-1, 1\}$. If $\alpha = \pm 1$, then $\langle 2, x \rangle$ generates the entire ring. But $3 \notin \langle 2, x \rangle$; hence, $\langle 2, x \rangle$ is not the entire ring. So, the ideal is not principal which means that $\mathbb{Z}[x]$ is not a PID.

# Euclidean Domains

We now introduce another algebraic domain that gives us properties of factorisation nicer than principal ideal domains.

# Euclidean Domains

We now introduce another algebraic domain that gives us properties of factorisation nicer than principal ideal domains.
Consider a domain $D$ and a function $\nu : D \to \mathbb{N}$ such that

for nonzero elements $f, g \in D$, $\nu(f) \leq \nu(fg)$, and

for any $f \in D$ and $g \in D \setminus \{0\}$, there exist $q, r \in D$ such that $f = gq + r$ with $r = 0$ or $\nu(r) < \nu(g)$.

# Euclidean Domains

We now introduce another algebraic domain that gives us properties of factorisation nicer than principal ideal domains.
Consider a domain $D$ and a function $\nu : D \to \mathbb{N}$ such that

> for nonzero elements $f, g \in D$, $\nu(f) \leq \nu(fg)$, and
>
> for any $f \in D$ and $g \in D \setminus \{0\}$, there exist $q, r \in D$ such that $f = gq + r$ with $r = 0$ or $\nu(r) < \nu(g)$.

If such a function exists, then $D$ is called a *Euclidean domain*.

# Euclidean Domains

We now introduce another algebraic domain that gives us properties of factorisation nicer than principal ideal domains.
Consider a domain $D$ and a function $\nu : D \to \mathbb{N}$ such that

> for nonzero elements $f, g \in D$, $\nu(f) \leq \nu(fg)$, and
>
> for any $f \in D$ and $g \in D \setminus \{0\}$, there exist $q, r \in D$ such that $f = gq + r$ with $r = 0$ or $\nu(r) < \nu(g)$.

If such a function exists, then $D$ is called a *Euclidean domain*.

It turns out that *every* Euclidean Domain is a PID (and hence, a UFD)!

# Euclidean Domains

We now introduce another algebraic domain that gives us properties of factorisation nicer than principal ideal domains.
Consider a domain $D$ and a function $\nu : D \to \mathbb{N}$ such that

> for nonzero elements $f, g \in D$, $\nu(f) \leq \nu(fg)$, and
>
> for any $f \in D$ and $g \in D \setminus \{0\}$, there exist $q, r \in D$ such that $f = gq + r$ with $r = 0$ or $\nu(r) < \nu(g)$.

If such a function exists, then $D$ is called a *Euclidean domain*.

It turns out that *every* Euclidean Domain is a PID (and hence, a UFD)!

So we have

$$\text{ED} \subseteq \text{PID} \subseteq \text{UFD}$$

## (2021, Q3 i)

Is $\mathbb{Z}[\sqrt{-5}]$ a Euclidean domain?

**(2021, Q3 i)**

Is $\mathbb{Z}[\sqrt{-5}]$ a Euclidean domain?

We showed that 21 did not factor uniquely. This implies that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. Since $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it is not a Euclidean domain.

# Gauss' Lemma I

We start with a definition.

## Primitive polynomials

Let $R$ be a UFD and consider some nonzero polynomial $f \in R[x]$. We say that $f$ is *primitive* if the coefficients are all coprime; that is, the greatest common divisor among the coefficients is 1.

# Gauss' Lemma I

We start with a definition.

## Primitive polynomials

Let $R$ be a UFD and consider some nonzero polynomial $f \in R[x]$. We say that $f$ is *primitive* if the coefficients are all coprime; that is, the greatest common divisor among the coefficients is 1.

For example, $f(x) = 3x^2 + 1 \in \mathbb{Z}[x]$ is a primitive polynomial.
However, $g(x) = 3x^2 + 6 \in \mathbb{Z}[x]$ is not.
Gauss' lemma is a powerful result about the product of such polynomials.

# Gauss' Lemma I

We start with a definition.

## Primitive polynomials

Let $R$ be a UFD and consider some nonzero polynomial $f \in R[x]$. We say that $f$ is *primitive* if the coefficients are all coprime; that is, the greatest common divisor among the coefficients is 1.

For example, $f(x) = 3x^2 + 1 \in \mathbb{Z}[x]$ is a primitive polynomial.
However, $g(x) = 3x^2 + 6 \in \mathbb{Z}[x]$ is not.
Gauss' lemma is a powerful result about the product of such polynomials.

## Gauss' lemma

Let $R$ be a UFD and suppose that $f$ and $f'$ are primitive polynomials in $R[x]$. Then the product $f \cdot f'$ is also primitive.

# Gauss' Lemma II

Consider some UFD, $R$. It turns out that the irreducible elements in $R[x]$ are:

irreducible elements of $R$ or

primitive polynomials of positive degree which are irreducible in $K[x]$ where $K$ is the fraction field of $R$.

# Gauss' Lemma II

Consider some UFD, $R$. It turns out that the irreducible elements in $R[x]$ are:

- irreducible elements of $R$ or
- primitive polynomials of positive degree which are irreducible in $K[x]$ where $K$ is the fraction field of $R$.

The above implies the following result.

Let $R$ be a UFD. Then $R[x]$ is a UFD.

# 6. Fields and Their Extensions

# Fields

We now place some more restrictions on the axioms of a ring. Let $R$ be a ring. Recall that

$R$ under addition is an abelian group.

$R$ is closed and associative under multiplication.

The operations are linked by the distributive properties.

For $R$ to be a field, we require the following conditions:

$R$ contains the multiplicative identity.

$R$ is commutative under multiplication.

Every element in $R$ has a multiplicative identity.

Then $R$ is a field. We usually denote this as $F$.

# Extensions of a field

Let $E$ be a field. What happens if I add in new elements into $E$? What sort of elements should I include for the bigger field to remain a field? We will formalise this.

# Extensions of a field

Let $E$ be a field. What happens if I add in new elements into $E$? What sort of elements should I include for the bigger field to remain a field? We will formalise this.

## Extension field

Let $E \subseteq F$ be a field. If $F$ is a field, then we call $F$ an extension field of $E$. We also say that $F/E$ a field extension.

# Extensions of a field

Let $E$ be a field. What happens if I add in new elements into $E$? What sort of elements should I include for the bigger field to remain a field? We will formalise this.

## Extension field

Let $E \subseteq F$ be a field. If $F$ is a field, then we call $F$ an extension field of $E$. We also say that $F/E$ a field extension.

Now imagine you have $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$. Then $E(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the smallest subfield of $F$ that contains $E, \alpha_1, \alpha_2, \ldots, \alpha_n$.
We call an extension *simple* if it is of the form $E(\alpha)$.

# Algebraic and transcendental elements

Let $E \subseteq F$ and consider some element $\alpha \in F$. We call $\alpha$ *algebraic* if $\alpha$ is a root of a (non-zero) polynomial $p$ with coefficients in $E$. By the First Isomorphism Theorem, $E[\alpha] \cong E[x]/\langle p \rangle$. We usually reserve $p$ to be irreducible – so that $p(x)$ is the minimal polynomial of $\alpha$.
Otherwise, $\alpha$ is said to be *transcendental*.

## (2016, Question 5 c)

Find the minimal polynomial of $\alpha = \sqrt{3 + 2\sqrt{2}}$ over $\mathbb{Q}$. Explain clearly how you know that the polynomial you have found is irreducible.

# Finite extensions and their degree I

Let $E \subseteq F$ be a field. Then $F$ can be viewed as a "vector space" over $E$ with the degree of the extension being the *dimension* of $F$ over $E$.

# Finite extensions and their degree II

Now suppose that $\alpha$ is algebraic over some field $F$. Then the degree of the extension field $F(\alpha)$ over $F$ is precisely the degree of the minimal polynomial; that is,

$$[F(\alpha) : F] = \deg p,$$

where $p$ is the minimal polynomial of $\alpha$ over $F$.
In fact, we can construct a tower of extensions. Suppose that $E \subseteq F \subseteq H$ all be fields. Then

$$[H : E] = [H : F] \cdot [F : E].$$

It might, however, be useful to know precisely when a polynomial over a field is irreducible.

# Irreducibility of polynomials – Eisenstein's criterion

Let $R$ be a unique factorisation domain with a fraction field $K$. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$. Suppose there exists some prime $p$ such that $p \mid a_0, a_1, \ldots a_{n-1}$ but $p \nmid a_n$ and $p^2 \nmid a_0$. Then $f$ is irreducible over $K$.

This gives us a sufficient condition to determine if $f$ is irreducible. But failure of the criterion does not guarantee that $f$ is *not* irreducible.

## (2020, Q5 ii)

Let $p \geq 3$ and define $\theta = 1 + \sqrt[p]{p} + \sqrt[p]{p^3} + \cdots + \sqrt[p]{p^{2p+1}}$. Find $[\mathbb{Q}(\theta) : \mathbb{Q}]$.

## (2020, Q5 ii)

Let $p \geq 3$ and define $\theta = 1 + \sqrt[p]{p} + \sqrt[p]{p^3} + \cdots + \sqrt[p]{p^{2p+1}}$. Find $[\mathbb{Q}(\theta) : \mathbb{Q}]$.

Observe that

$$\mathbb{Q} \subseteq \mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt[p]{p}).$$

## (2020, Q5 ii)

Let $p \geq 3$ and define $\theta = 1 + \sqrt[p]{p} + \sqrt[p]{p^3} + \cdots + \sqrt[p]{p^{2p+1}}$. Find $[\mathbb{Q}(\theta) : \mathbb{Q}]$.

Observe that

$$\mathbb{Q} \subseteq \mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt[p]{p}).$$

We, therefore, have that

$$[\mathbb{Q}(\theta) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[p]{p}) : \mathbb{Q}].$$

By Eisenstein's criterion on $p$, we claim that $x^p - p$ is the minimal polynomial of $\sqrt[p]{p}$ over $\mathbb{Q}$. In other words, we have that

$$[\mathbb{Q}(\theta) : \mathbb{Q}] \mid p \implies [\mathbb{Q}(\theta) : \mathbb{Q}] = \{1, p\} \implies [\mathbb{Q}(\theta) : \mathbb{Q}] = p.$$

# Splitting fields I

# Splitting fields I

Let $f(x) = x^2 - 8$.

# Splitting fields I

Let $f(x) = x^2 - 8$. If we consider this polynomial over $\mathbb{Q}$, then $f$ is irreducible because the roots $\sqrt{8}$ and $-\sqrt{8}$ do not belong in $\mathbb{Q}$.

# Splitting fields I

Let $f(x) = x^2 - 8$. If we consider this polynomial over $\mathbb{Q}$, then $f$ is irreducible because the roots $\sqrt{8}$ and $-\sqrt{8}$ do not belong in $\mathbb{Q}$. But if we consider this polynomial over $\mathbb{Q}(\sqrt{2})$, then certainly $f$ can be factored into

$$f(x) = (x - 2\sqrt{2})(x + 2\sqrt{2})$$

and each of these coefficients belong in $\mathbb{Q}(\sqrt{2})$.

# Splitting fields I

Let $f(x) = x^2 - 8$. If we consider this polynomial over $\mathbb{Q}$, then $f$ is irreducible because the roots $\sqrt{8}$ and $-\sqrt{8}$ do not belong in $\mathbb{Q}$. But if we consider this polynomial over $\mathbb{Q}(\sqrt{2})$, then certainly $f$ can be factored into

$$f(x) = (x - 2\sqrt{2})(x + 2\sqrt{2})$$

and each of these coefficients belong in $\mathbb{Q}(\sqrt{2})$. We call $\mathbb{Q}(\sqrt{2})$ the *splitting field* of $f$ because it splits $f$ into linear factors.

# Splitting fields II

More generally,

**Splitting field**

Let $F$ be a field. A *splitting field* of some polynomial $p(x)$ over $F$ is an extension field $K$ such that $p$ splits into linear factors.

We generally restrict ourselves to the *smallest* field for which this happens and call this *the splitting field* of $p$.

## Kronecker

Let $F$ be a field and consider $f \in F[x]$. Then there exist a finite extension $E/F$ such that $f$ is a product of linear factors in $E[x]$; that is,

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n),$$

where $\alpha_1, \alpha_2, \dots, \alpha_n \in E$.

## Kronecker

Let $F$ be a field and consider $f \in F[x]$. Then there exist a finite extension $E/F$ such that $f$ is a product of linear factors in $E[x]$; that is,

$$f(x) = a(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n),$$

where $\alpha_1, \alpha_2, \dots, \alpha_n \in E$.

What this tells us is that, we can generate the splitting field as follows:

## Kronecker

Let $F$ be a field and consider $f \in F[x]$. Then there exist a finite extension $E/F$ such that $f$ is a product of linear factors in $E[x]$; that is,

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n),$$

where $\alpha_1, \alpha_2, \dots, \alpha_n \in E$.

What this tells us is that, we can generate the splitting field as follows:

- Find the roots of $f$. The splitting field must contain all of the roots of $f$.

## Kronecker

Let $F$ be a field and consider $f \in F[x]$. Then there exist a finite extension $E/F$ such that $f$ is a product of linear factors in $E[x]$; that is,

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n),$$

where $\alpha_1, \alpha_2, \dots, \alpha_n \in E$.

What this tells us is that, we can generate the splitting field as follows:

- Find the roots of $f$. The splitting field must contain all of the roots of $f$.
- If the field $F$ contains any of the roots, then we don't need to consider them in the field extension. Otherwise, adjoin the element so that the field extension now contains all linear combinations of the root. Repeat this until we include all of the roots. The resulting field is the *splitting field* of $f$.

## (2021, Question 5 ii)

Find the splitting field of the polynomial $f(x) = x^3 - 11$ over $\mathbb{Q}$ and compute the degree of its extension over $\mathbb{Q}$.

## (2021, Question 5 ii)

Find the splitting field of the polynomial $f(x) = x^3 - 11$ over $\mathbb{Q}$ and compute the degree of its extension over $\mathbb{Q}$.

Recall that its splitting field separates the polynomial into linear factors. This means that the splitting field must contain all of its roots. The roots of $f(x)$ are $\{\sqrt[3]{11}, \sqrt[3]{11}\xi, \sqrt[3]{11}\xi^2\}$ where $\xi$ denotes the primitive root of degree 3. The splitting field, therefore, becomes $\mathbb{Q}(\sqrt[3]{11}, \xi)$.

## (2021, Question 5 ii)

Find the splitting field of the polynomial $f(x) = x^3 - 11$ over $\mathbb{Q}$ and compute the degree of its extension over $\mathbb{Q}$.

Recall that its splitting field separates the polynomial into linear factors. This means that the splitting field must contain all of its roots. The roots of $f(x)$ are $\{\sqrt[3]{11}, \sqrt[3]{11}\xi, \sqrt[3]{11}\xi^2\}$ where $\xi$ denotes the primitive root of degree 3. The splitting field, therefore, becomes $\mathbb{Q}(\sqrt[3]{11}, \xi)$.
To determine its degree, we can compute the tower of extensions

$$[\mathbb{Q}(\sqrt[3]{11}, \xi) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{11})(\xi) : \mathbb{Q}(\sqrt[3]{11})] \cdot [\mathbb{Q}(\sqrt[3]{11}) : \mathbb{Q}].$$

The minimal polynomial of $\mathbb{Q}(\sqrt[3]{11}, \xi)$ over $\mathbb{Q}(\sqrt[3]{11})$ has degree 2 while the minimal polynomial of $\mathbb{Q}(\sqrt[3]{11})$ over $\mathbb{Q}$ has degree 3. Thus, $\mathbb{Q}(\sqrt[3]{11}, \xi)$ is an extension of degree $2 \times 3 = 6$.

# Finite fields

Let $F$ be a field. We call $F$ a *finite field* if it has finitely many elements. In fact, if $F$ is a finite field, then $|F| = p^n$ for some integer $n \geq 1$ and $p \geq 2$ prime. The prime $p$ is called the *characteristic* of $F$.
If $F$ is a field of $q = p^n$ elements, then $F^*$ is a cyclic group of order $q - 1$. Note that the only element that doesn't have a multiplicative inverse is the 0 element.

# Finite fields

**(2020, Q4 iii)**

Prove that the rings $(\mathbb{Z}/3\mathbb{Z})[x]/(x^2+x+2)$ and $(\mathbb{Z}/3\mathbb{Z}[x])/(x^2+2x+2)$ are isomorphic.

## (2015, Question 5)

Consider the following rings, each of which has 9 elements:

- $\mathbb{Z}/9\mathbb{Z}$,
- $\mathbb{F}_9$,
- $\mathbb{F}_3 \times \mathbb{F}_3$,
- $\mathbb{F}_3[x]/(x^2)$,
- $\mathbb{F}_3[x]/(x^2+1)$,
- $\mathbb{F}_3[x]/(x^2-1)$.

Sort these rings into equivalence classes under the relation "$R$ is isomorphic to $S$".