Groups and Symmetries Notes

Francesco Chotuck

Abstract

This is KCL undergraduate module 5CCM232A, instructed by Dr Paul P. Cook. The formal name for this class is "Groups and Symmetries".

Contents

1 Basics

Definition 1.1. A **group** is a set G and a mapping from the Cartesian product $G \times G$ into G which will we denote by juxtaposition (variables side by side)

$$G \times G \to G$$
$$(g_1, g_2) \mapsto g_1 g_2,$$

with the following properties:

- Associativity: $g_1(g_2 g_3) = (g_1 g_2)g_3$ for all $g_1, g_2, g_3 \in G$;
- Identity: there exists $e \in G$, called an identity, such that $ge = eg = g$ for all $g \in G$;
- Inverse: for all $g \in G$ there exists $g^{-1} \in G$, called an inverse of g, such that $gg^{-1} = g^{-1}g = e$, where e is an identity in G.

> **Remark 1.1.** When asked to define a group state this: "a group is a set with a multiplication law $G \times G \to G$ with $(g_1, g_2) \mapsto g_1 g_2$ which satisfies etc...".

Elements in groups have some "nice" properties:

1. The identity e is unique;
2. Given any $g \in G$ its inverse g^{-1} is unique;
3. $(gh)^{-1} = h^{-1}g^{-1}$ for all $g, h \in G$;
4. $(g^{-1})^{-1} = g$ for all $g \in G$.

Definition 1.2. The order of a group G is the number of elements of G, denoted $|G|$.

Definition 1.3. If $gh = hg$ for all $g, h \in G$, then G is a **commutative**, or **abelian**, group.

Definition 1.4. A subset $H \subset G$ is a subgroup of G if it is a group under the law of composition of G. That is, H is a subgroup if

1. $h_1 h_2 \in H$ for all $h_1, h_2 \in H$ and
2. $h^{-1} \in H$ for all $h \in H$.

Example 1.1

Some interesting examples of groups are:

- $\mathbb{Z}_p$: the integers under addition modulo $p \in \mathbb{N}$;
- Matrices with determinant 1 under the matrix multiplication (determinant of 1 is necessary to guarantee the existence of inverses);

Note 1.1. In this course the set $\mathbb{R}^* = \mathbb{R}\backslash 0$.

2 The Cyclic Groups

Let $g \in G$ be an element of a group G which has identity e. The power notation for group elements g^n where $n \in \mathbb{Z}$ is defined to be the n-times product of g with itself i.e. $\underbrace{gg\dots g}_{n \text{ times}}$, for $n > 0$; it is the $|n|$-times product of g^{-1} with itself for $n < 0$, and it is e if $n = 0$. Consequently, we define

$$g^{m+n} = g^m g^n, \quad (g^m)^n = g^{mn} \quad \forall m, n \in \mathbb{Z}.$$

Definition 2.1. A group G is called **cyclic** if there is exists a $g \in G$ such that $G = \langle g \rangle$. Such an element is called a **generating element** for G; in general it is **not** unique.

Theorem 2.1. The set generated by $g \in G$, denoted $\langle g \rangle$, is the set of all powers if g:

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

Note 2.1. All cyclic groups are abelian.

Theorem 2.2. If p is prime then $\mathbb{Z}_p = \langle n \rangle$ for any $n \in \{1, 2, 3, \dots, p-1\}$.

Theorem 2.3. Let G be a cyclic group generated by g_0. Then

1. g_0^n for $n = 0, 1, 2, \dots, |G| - 1$ are all **distinct** elements and
2. $g^{|G|} = e$ for all $g \in G$.

Theorem 2.4. Every subgroup of a cyclic group is cyclic.

2.1 Symbols and relations

The notion of a generating element can be extended to more than one element. Let $\langle a, b \rangle$ is the set of all powers of a and b and their products i.e.

$$\langle a, b \rangle = \{e, a, a^2, \dots, b, b^2, \dots, ab, ab^2, \dots, ba, ba^2, \dots, abab, \dots\}$$

is called the span of a and b, or the group generated by a and b. By imposing restriction such as $a^n = e, b^n = e$ and $a^n b^n = b^n a^n$ for any $n \in \mathbb{Z}$ the span of a and b becomes a finite set which allows us to denote a group.

3 Maps and Permutation Groups

Consider two sets X, Y and a map $f : X \to Y$. We write $y = f(x)$ for the value in Y that is mapped from $x \in X$.

Definition 3.1. We say y is the **image** of x under f.

Definition 3.2. The set $f(X) = \{f(x) : x \in X\} \subset Y$ is the image of X under f.

Definition 3.3. The map f is **surjective** (or **onto**) if every $y \in Y$ is the image of at least one $x \in X$ i.e. if $f(X) = Y$ (denoted $f : X \twoheadrightarrow Y$).

Definition 3.4. The map f is **injective** (or **one-to-one**) if for all $y \in f(X)$ there exists a **unique** $x \in X$ such that $y = f(x)$ (denoted $f : X \rightarrowtail Y$).

Proposition 3.1. A function is said to be injective if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$.

Definition 3.5. A map f that is both injective and surjective is said to be **bijective**.

Theorem 3.1. If $f : X \to Y$ is bijective an **inverse** map $f^{-1} : Y \to X$ can define such that

$$f(f^{-1}(y)) = y, \quad f^{-1}(f(x)) = x \quad \forall y \in Y, x \in X.$$

Remark 3.1. The inverse map itself is bijective.

Theorem 3.2. The span of a set of bijective maps of a finite set X to itself forms a group under composition of maps. This is called a **permutation group** of X, $\mathrm{Perm}(X)$.

Definition 3.6. The set of all permutations of a finite set containing n elements is called the **symmetric group** S_n.

Note 3.1. The set $\mathrm{Perm}(X) \in S_{|X|}$.

Theorem 3.3. The order of the symmetric group $|S_n|$ is $n!$.

Example 3.1

S_3 is a symmetric group of all permutations of three elements. It consists of the permutations:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = a, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = a^2,$$
$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = b, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = a^2b, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = ab,$$

Notice how the bottom row is cycled through by 'shifting to the right' i.e. bottom row for $e = (123), a = (231), a^2 = (312)$ and so on.

Remark 3.2. A 2-cycle such as (12) is called a **transposition** and every permutation can be rewritten as a product of a transposition. The converse is also true i.e. every cycle permutation can be rewritten as a transposition.

Definition 3.7. An **even permutation** is one which can be written as the product of an even number of transposition.

Definition 3.8. An **odd permutation** is one which can be written using an odd number of transposition.

Definition 3.9. The **alternating group** A_n is a subgroup of S_n consisting of all the even permutations in S_n.

Theorem 3.4. The order of A_n is always half the permutations in S_n, hence $|A_n| = \frac{n!}{2}$.

3.1 Cycle composition

Definition 3.10. Two (or more) cycles are **disjoint** if they do not have any common elements.

Theorem 3.5. Every permutation $\sigma \in S_n$ can be decomposed to a composition of **disjoint cycles**.

Example 3.2

Let $\sigma = (173)(15) \in S_7$. Write the decomposition of σ into disjoint cycles.
Solution: The cycles (173) and (15) are **NOT** disjoint since they both share the element 1.
Let $\sigma = \underbrace{(173)}_{\alpha}\underbrace{(15)}_{\beta} = \alpha\beta$. Then

$$\begin{aligned}
\sigma(1) &= \alpha\beta(1) = \alpha(\beta(1)) = \alpha(5) = 5\\
\sigma(2) &= \alpha\beta(2) = \alpha(\beta(2)) = \alpha(2) = 2\\
\sigma(3) &= \alpha\beta(3) = \alpha(\beta(3)) = \alpha(3) = 1\\
\sigma(4) &= \alpha\beta(4) = \alpha(\beta(4)) = \alpha(4) = 4\\
\sigma(5) &= \alpha\beta(5) = \alpha(\beta(5)) = \alpha(1) = 7\\
\sigma(6) &= \alpha\beta(6) = \alpha(\beta(6)) = \alpha(6) = 6\\
\sigma(7) &= \alpha\beta(7) = \alpha(\beta(7)) = \alpha(7) = 3.
\end{aligned}$$

So, $\sigma = (1573)$.

4 Homomorphism and Isomorphism

Definition 4.1. Let G and H be groups. A map $\phi : G \to H$ is a **homomorphism** (of groups) if $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in G$.

Remark 4.1. The operation on the LHS is the operation of the group G, whereas the operation on the RHS is that of group H; i.e.

$$\phi(g \underbrace{\circ}_{\text{in } G} h) = \phi(g) \underbrace{\circ}_{\text{in } H} \phi(h).$$

Note 4.1. For a group homomorphism given by ϕ note that

- the notation $\phi^{-1}(g)$ means the **inverse map** of ϕ whereas,
- the notation $(\phi(g))^{-1}$ means the **inverse element** of $\phi(g)$.

Theorem 4.1. Let ϕ be a homomorphism from G to H and e_G, e_H be the identity elements in G and H respectively, then

1. $\phi(e_G) = e_H$ and
2. $\phi(g^{-1}) = (\phi(g))^{-1}$ for all $g \in G$

Proof. We prove each statement in turn.

1. Since $e_G e_G = e_G$ then, $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$. Multiplying by the inverse element $(\phi(e_G))^{-1}$ in H, and we have $\phi(e_G)\phi(e_G)^{-1} = \phi(e_G)\phi(e_G)\phi(e_G)^{-1}$ hence, $e_H = \phi(e_G)$.
2. Consider $e_G = gg^{-1}$ for $g \in G$ then, using the previous result we have $e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$. Multiplying by the inverse element $\phi(g)^{-1}$ in H we have $\phi(g)^{-1} = \phi(g)^{-1}\phi(g)\phi(g^{-1}) = \phi(g^{-1})$.

□

Note 4.2. If we want to check whether if two groups are homomorphic we need to check whether Definition 4.1 and Theorem 4.1 hold.

Definition 4.2. An **isomorphism** is a homomorphism that is bijective.

Example 4.1. A trivial example of an isomorphism is the identity map $\mathrm{id} : G \to H$.

Definition 4.3. Two groups G and H are **isomorphic** if there exists an isomorphism $\phi : G \to H$.

Theorem 4.1

The 'isomorphic' relation is an equivalence relation, denoted by $\cong$.

Remark 4.2. If two groups are isomorphic then they are structurally the same group; i.e. if $G \cong H$ then: $|G| = |H|$; G abelian $\iff$ H abelian; etc.

Theorem 4.2. The **order of an element** $g \in G$ is the smallest positive integer k such that $g^k = e$.

Corollary 4.1. Let $\phi : G \to H$ be an isomorphism and let $g \in G$ then $\phi(g^n) = (\phi(g))^n$.

Theorem 4.2

Two cyclic groups of the same order are isomorphic.

Proof. Let $G = \langle g \rangle$ and $H = \langle h \rangle$ with $N = |G| = |H|$ where N is finite. Since, G and H are cyclic groups we can write

$$G = \{g^0, g^1, g^2, \ldots, g^{N-1}\} \quad \text{and} \quad G = \{h^0, h^1, h^2, \ldots, h^{N-1}\}$$

as sets. Define the map

$$\begin{aligned} \phi : G &\to H \\ \phi(g^n) &\mapsto h^n \end{aligned}$$

fot all $n \in \mathbb{Z}$. We will show that this is an isomorphism. By contruction it is bijective. To show it is a homomorphism, consider

$$\begin{aligned} \phi(g^m g^n) &= \phi(g^{m+n}) \\ &= h^{m+n} \\ &= h^m h^n \\ &= \phi(g^m)\phi(g^n). \end{aligned}$$

□

5 Cosets and Lagrange's theorem

Let $H \subset G$ be a subgroup of the group G. We can define an equivalence relation between $a, b \in G$ if they are related by **left multiplication** by an element of H, i.e. if

$$ha = b \quad \text{then} \quad ba^{-1} = h \in H \quad \text{for some } h \in H.$$

So we define an equivalence relation $\sim$ by:

$$a \sim b \iff ba^{-1} \in H.$$

Example 5.1

Consider the group

$$G = \left\{ \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} : a \in \mathbb{R},\ a \neq 0,\ b \in \mathbb{R} \right\}.$$

Let

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R},\ a \neq 0 \right\}$$

be a subgroup of G. Find matrices which, up to equivalence, form the left-coset space G/H.

Solution. Recall, two elements $M, N \in G$ lie in the same left coset with respect to H if $M^{-1}N \in H$. Let

$$M = \begin{pmatrix} a_1 & 0 \\ b_1 & a_1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a_2 & 0 \\ b_2 & a_2 \end{pmatrix}$$

then,

$$M^{-1} = \frac{1}{a_1} \begin{pmatrix} 1 & 0 \\ -\frac{b_1}{a_1} & 1 \end{pmatrix}.$$

We want

$$\begin{aligned} M^{-1}N &= \begin{pmatrix} 1 & 0 \\ -\frac{b_1}{a_1} & 1 \end{pmatrix} \begin{pmatrix} a_2 & 0 \\ b_2 & a_2 \end{pmatrix} \\ &= \frac{1}{a_1} \begin{pmatrix} a_2 & 0 \\ -\frac{b_1 a_2}{a_1} + b_2 & a_2 \end{pmatrix} \in H. \end{aligned}$$

Therefore, we must have $-\frac{b_1 a_2}{a_1} + b_2 = 0$ which implies

$$\frac{b_1}{a_1} = \frac{b_2}{a_2} \equiv \lambda \in \mathbb{R}.$$

Setting $a_1 = 1$ gives

$$G/H = \left\{ \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} : \lambda \in \mathbb{R} \right\}.$$

Definition 5.1. The **equivalence class** of a is denoted by $[a] := \{b \in G : b \sim a\}$.

Denote the set $Ha := \{ha : h \in H\}$ then, this will be shown as $[a] = Ha = \{e, h_1, h_2, \ldots, h_{n-1}\}a = \{a, h_1 a, h_2 a, \ldots, h_{n-1}a\}$, (supposing the set has n elements).

Definition 5.2. The set of equivalence classes $Ha = [a] = \{Ha : a \in G\}$ is the set of **right cosets** of G with respect to H, where G is a group and $H \subset G$ is a subgroup of G.

Definition 5.3. The set of equivalence classes $\{aH : a \in G\}$ is the set of **left cosets** of G with respect to H.

> **Remark 5.1.** For left cosets we define the equivalence relation as $a \sim b$ if and only $ah = b$ for some $h \in H$. Or equivalently $a \sim b$ if and only if $a^{-1}b \in H$.

Theorem 5.1. Two right cosets of G with respect to H are either **disjoint** or **identical**.

Proof. Let $a, b \in G$. If $[a]$ and $[b]$ have no elements in common, then they are disjoint. If $c \in [a]$ and $c \in [b]$, then $a \sim c$ and $b \sim c$, hence $a \sim b$ by transitivity and symmetry therefore, $[a] = [b]$. □

> **Note 5.1.** When listings cosets if one the cosets has **at least** on element in common with another coset then stop listing, as such coset is identical to one listed before.

Theorem 5.2. All right cosets of G with respect to H have the same number of elements.

Proof. It is enough to show there is a bijection between two right cosets.
Fix $g \in G$ and consider its right coset Hg. Consider the map

$$\begin{aligned} M : H &\to Hg \\ h &\mapsto hg. \end{aligned}$$

We now show it's a bijective map. Given $a \in Hg$ we have $a = hg$ for some $h \in H$ hence, $a = M(g)$ so, M is surjective. Suppose $M(h) = M(h')$ then $hg = h'g$ hence, $hgg^{-1} = h'gg^{-1} \Rightarrow h = h'$ so, M is injective. □

> **Note 5.2.** In mathematics when wanting to prove two sets have the same cardinality it is enough to show that there is a bijection between the two sets.

Definition 5.4. The number of cosets of G with respect to H is called the **index** of H in G, which is denoted by $i(H, G)$.

> **Theorem 5.1** (Lagrange's Theorem)
> Let H be a subgroup of G. The order of H divides the order of G i.e.
>
> $$|G| = |H|\, i(H, G).$$

Definition 5.5. A **proper subgroup** of G is a subgroup $H \subset G$ that is different from the trivial group $\{e\}$ and from G itself.

Corollary 5.1. If $|G|$ is prime, then the group G has no proper subgroup.

Proof. For the sake of contradiction, suppose H is a proper subgroup of G then, $|H|$ divides $|G|$ however, $|H|$ is a number not equal to 1 or $|G|$. □

Corollary 5.2. Let $g \in G$ and let k be the order of g. Then k divides $|G|$.

Proof. The order of g is the same as the order of $\langle g \rangle$, the subgroup of G generated by g. By applying Lagrange's theorem on $\langle g \rangle$ we conclude that the order of g divides the order of G. □

Corollary 5.3. If $|G|$ is prime then G is a cyclic group.

Proof. Given any $g \in G$ where $g \neq e$, consider the subgroup $\langle g \rangle$. Since $|G|$ is prime it has no proper subgroups. Since the order of $\langle g \rangle$ is greater than 1 then $\langle g \rangle$ must be G itself. □

6 Groups of Low order

We will identify or construct all the groups of low order.

- $|G| = 1 \Rightarrow G = \{e\}$. This is the only possibility as e must always be contained in the group.
- $|G| = 2 \Rightarrow G = \{e, a\}$. With $a \neq e$, as G is a group then a^{-1} exists and is $a^{-1} = a \Rightarrow a^2 = e$. Since the order of G is 2, that is prime then we have $G \cong \mathbb{Z}_2$.
- $|G| = 3 \Rightarrow G = \{e, a, b\}$. As $|G|$ is prime then $G \cong \mathbb{Z}_3$.
- $|G| = 4 \Rightarrow G = \{e, a, b, c\}$

Theorem 6.1. Every group of order 4 is either cyclic or has the rules:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Note 6.1. In a Cayley table there are no repeat entries in a row and column.

Remark 6.1. If Cayley table is symmetric i.e. switch the rows with column then the group is abelian.

6.1 The Klein's Four Group

Definition 6.1. The group with the rules above is denoted V_4 and called the **Klein four-group** (Vieregruppe).

Theorem 6.1

The group V_4 can be described using symbols and relations. It is generated by the symbols a, b with the relations $a^2 = b^2 = e$ and $ab = ba$. So we have

$$V_4 = \langle a, b \rangle = \{e, a, b, ab\}.$$

Proposition 6.1. All groups of order 5 or less are abelian.

Proposition 6.2. Properties of V_4:

1. it is the smallest non-cyclic group;
2. All the elements have order 2 (for exception to the identity);
3. it has 5 subgroups: the trivial ones as well as the 3 proper subgroups, $\langle a \rangle, \langle b \rangle$ and $\langle ab \rangle$.

Theorem 6.2. The group V_4 can be seen as a subgroup of S_4:

$$\left\{e, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}.$$

Proposition 6.3. $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

7 Direct Products

Definition 7.1. Let G and H be groups. Then $G \times H = \{(g, h) : g \in G, h \in H\}$ is a group, with the multiplication law $(g, h)(g', h') = (gg', hh')$. We call $G \times H$ the **direct product** of G and H.

Proposition 7.1. If G and H are abelian then so is $G \times H$.

Proposition 7.2. The order of $G \times H$ is $|G \times H| = |G|\,|H|$.

Theorem 7.1
A group of order 6 is isomorphic to $\mathbb{Z}_6$ (the cyclic group of order 6) or to S_3.

Example 7.1. Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_3$; this group has order 6. Is this group isomorphic to $\mathbb{Z}_6$ or S_3? We note that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is abelian and so is $\mathbb{Z}_6$ however S_3 is not. Hence, we conclude that

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6.$$

Theorem 7.2
The group $\mathbb{Z}_p \times \mathbb{Z}_q$ is isomorphic to $\mathbb{Z}_{pq}$ if and only if p and q are coprime.

Lemma 7.1. All groups of even order contain at least one non-identity element whose order is 2.

Proof. Consider a finite group of even order where $G = \{e, g_1, g_2, \ldots, g_{2n-1}\}$ for $n \in \mathbb{Z}$. For the sake of contradiction, suppose that G does not contain any non-identity element of order 2 and note that such an element is its own inverse element. We can pair up each element with its unique inverse element. But, e is its own inverse element which means that we have an odd number of remaining elements to be ordered into distinct pairs – which cannot be done. Hence, the assumption is contradicted. □

Example 7.2.

- Consider the group $\mathbb{Z}_2 = \{e, a\}$, it has $a^2 = e$;
- the group $\mathbb{Z}_4 = \{e, a, a^2, a^3\}$ has $(a^2)^2 = e$.

8 Symmetry transformations

8.1 Symmetries and groups

Definition 8.1. A **symmetry transformation** is an action on a set that leaves the set as a whole **unaltered**.

Note 8.1. An even function $f(x)$ has the property $f(x) = f(-x)$, it is symmetric under the map $x \mapsto -x$. In $\mathbb{R}^2$ this is a symmetric reflection in the y-axis. An odd function satisfies $g(x) = -g(-x)$, and it is symmetric reflection about the origin.

8.2 Isometries of the Euclidean Plane

Definition 8.2. Let X and Y be two vector spaces equipped with distance functions D_X and D_Y. An isometry between X and Y is a distance preserving map $f : X \to Y$ i.e.

$$D_X(x_1, x_2) = D_Y(y_1, y_2)$$

where $f(x_1) = y_1$ and $f(x_2) = y_2$.

The transformations of $\mathbb{R}^2$ can be described with matrices:

- an anti-clockwise rotation of θ about the origin is given by

$$A(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

  Its inverse is given by

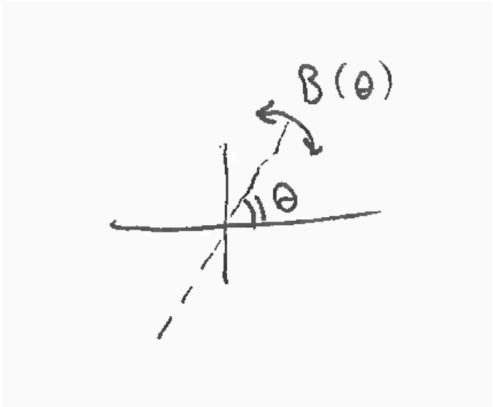
$$A(-\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix};$$

- a reflection in the straight line through the origin at angle θ to the x-axis is

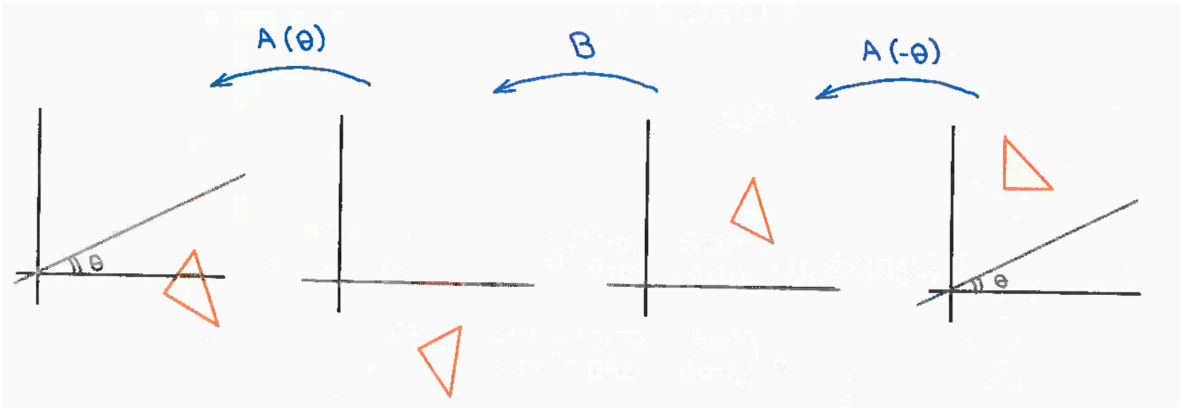
$$B(\theta) = A(\theta)BA(-\theta)$$

  where B is a reflection in the x-axis, so $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ i.e. $B \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -y \end{pmatrix}$.

Geometrically the operation $B(\theta)$ is a reflection on the straight line inclined by θ as indicated in the figure below.



Similarly consider the operation $B(\theta) = A(\theta)BA(-\theta)$, we do the operation from right to left. We will explain the geometric interpretation with the aid of the diagram below.



Consider the straight line through the origin inclined at θ and a triangle which we want to apply $B(\theta)$:

1. we rotate the line down to the x-axis with $A(-\theta)$;
2. then apply a reflection on the x-axis with B;
3. restore the line by moving back by θ with $A(\theta)$.

Proposition 8.1

The properties of $A(\theta)$ and $B(\theta)$:

- $A(\theta + \pi) = -A(\theta)$;
- $B(\theta + \pi) = B(\theta)$;
- $A(\theta)BA(\theta) = B \Rightarrow A(\theta)B = BA(-\theta)$;
- $(A(\theta))^\top = A(-\theta)$;
- $B^\top = B$;
- $(B(\theta))^\top = B(\theta)$.

Definition 8.3. Let $n \geq 2$ be an integer. The set of rotations and reflections that preserve the regular n-sided polygon P_n is called **dihedral group**, D_n.

Theorem 8.1

Let $n \geq 2$ be an integer. The set of rotations and reflections that preserve the regular polygon P_n, formed by successively joining the points

$$\begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) \end{pmatrix}, \; k = 0, 1, \ldots, n-1$$

by straight lines, is called the **dihedral group** D_n.

Remark 8.1. The case $n = 2$ is a special case: P_2 is a line segment and not a polygon. We have that $D_2 \cong V_4$.

Proposition 8.1. The order of the groups D_n is given by $|D_n| = 2n$.

Theorem 8.2

The full set of the dihedral group elements is:

$$D_n = \langle a, b \rangle = \{\underbrace{e, a, a^2, \ldots, a^{n-1}}_{n \text{ rotations}}, \underbrace{b, ab, a^2b, \ldots, a^{n-1}b}_{n \text{ reflections}}\}$$

equipped with $a^n = e, b^2 = e$ and $a^k b = ba^{-k}$ as

$$\underbrace{\left(A\left(\frac{2\pi}{n}\right)\right)^k B}_{a^k b} = A\left(\frac{2\pi k}{n}\right) B = BA\left(-\frac{2\pi k}{n}\right) = \underbrace{B\left(A\left(-\frac{2\pi}{n}\right)\right)^k}_{ba^{-k}}.$$

Remark 8.2. We have that $D_3 \cong S_3$.

Corollary 8.1. A combination of rotations and reflection can always be represented by a reflection.

Corollary 8.1

The order of every reflection is 2.

9 Conjugation, Normal Subgroups and Quotient Groups

9.1 Conjugation

Definition 9.1. Given a group G, we sat that a is **conjugate** to b if there exists a $g \in G$ such that $a = gbg^{-1}$ for $a, b \in G$.

Remark 9.1. Every finite group G is made up of some set of permutation in the symmetric group, if $|G| = n$ then we can embed G into S_n i.e. $G \subset S_{|G|}$. This is known as **Cayley's theorem** which can be restated as: every group G is isomorphic to a subgroup of a symmetric group.

Note 9.1. We can interpret conjugation as changing labels of the elements.

Example 9.1. Conjugation in the symmetric group relates the permutations formed out of the same length cycles where the only difference is that the labels in the cycles are change. Thus, conjugation is a way of relating similar transformations. Consider the permutation $(123) \in S_3$. If we swapped the labels of the elements $2 \leftrightarrow 3$ we would find another 3-cycle permutation, namely (132). We can carry out the swap $2 \leftrightarrow 3$ using elements of S_3 as follows:

$$(23)(123)(23)^{-1} = (23)(123)(23) = (132).$$

The operation $(23)(123)(23)$ is a conjugation of (123) with $g = (23)$.

Theorem 9.1. The conjugacy relation is an equivalence relation.

Definition 9.2. The set $[a]_C = \{gag^{-1} : g \in G\}$ is called the **conjugacy class** of a.

Proposition 9.1
Two or more conjugacy classes are either disjoint or identical.

Remark 9.2. Conjugation is an equivalence relation.

Theorem 9.2. Conjugacy classes form a partition of G however, it is **not** an equipartition.

Proposition 9.1. Properties of conjugacy classes:

- $[e]_C = \{e\}$ hence, no other class is a subgroup as the identity element is not contained in all classes.
- All elements of a conjugacy class have the same order.
- If G is abelian then $[a]_C = \{a\}$ for all $a \in G$.

Corollary 9.1. Suppose G is a group and $a, b, g \in G$. Let $b = gag^{-1}$ then $b^k = ga^kg^{-1}$; i.e. the order is preserved.

Corollary 9.1

Suppose G is a group then all elements of G in the same conjugacy class are elements of the same order.

Proof. Suppose that the order of $a \in G$ is k i.e. $a^k = e$. Consider an element $b \in [a]_C$, i.e. $b \sim a \Rightarrow b = gag^{-1}$. We have that $b^n = ga^n g^{-1}$, the lowest value of n for which $b^n = e$ is when $n = k$, the order of a, i.e. $b^k = ga^k g^{-1} = geg^{-1} = gg^{-1} = e$. Hence, all elements in the same conjucacy class have the same order. □

Proposition 9.2. If G is an abelian group then $[a]_C = \{a\}$ for all $a \in G$.

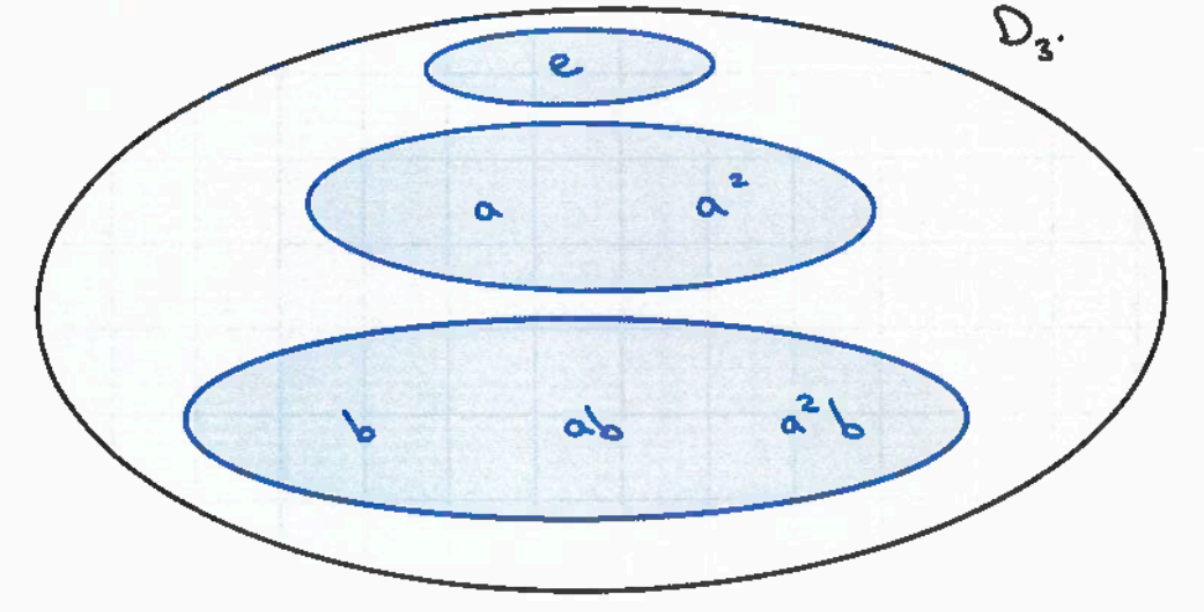
Proof. As $[a]_C = \{gag^{-1} \mid \forall a \in G\} = \{gg^{-1}a \mid \forall g \in G\} = \{a\}$. □

Theorem 9.3. On any subset $H \subset G$, the conjugation map

$$\begin{aligned} M : H &\mapsto gHg^{-1} \\ h &\mapsto ghg^{-1} \end{aligned}$$

associated to $g \in G$ is bijective.

Example 9.2. In this example we illustrate how the group D_3 is partitioned in respect to its conjugacy classes. Notice how it is not an equipartition.



Example 9.1

Consider $D_3 \cong S_3$. We know $D_3 = \langle a, b \rangle$ with $a^3 = e, b^2 = e$ and $ab = ba^{-1} = ba^2$ so, $D_3 = \{e, a, a^2, b, ab, a^2b\}$. Let us look at the order of each element:

$$D_3 = \{\underbrace{e}_{1}, \underbrace{a, a^2}_{3}, \underbrace{b, ab, a^2b}_{2}\}.$$

Firstly, by Proposition 9.1 we have our first conjugacy class,

$$[e]_C = \{e\};$$

secondly we have that all elements in a conjugacy class have the same order thus, we can guess that the conjugacy classes could be

$$[a]_C = \{a, a^2\} \quad \text{and} \quad [b]_C = \{b, ab, a^2b\}.$$

Now we need to check if they are conjugacy classes:

- $[a]_C$ can only contain a and a^2; by definition a is contained in its conjugacy class, so we need to check if $a^2 \in [a]_C$. We can split the elements of D_3 (in general D_n) into rotations and reflections i.e. a^n and a^nb. Now check if a^2 can be conjugated by rotations and reflections:

$$a^n a^2 a^{-n} = a^2 \checkmark$$
$$(a^n b)a^2(a^n b)^{-1} = (a^n b)a^2(ba^{-n}) = a^2. \checkmark$$

  We conclude that $a^2 \in [a]_C$.

- Similarly, we need to check if $ab, a^2b \in [b]_C$; as before $b \in [b]_C$ by definition of a conjugacy class. So, check if b can be conjugated by rotations and reflections:

$$a^n b a^{-n} = a^{2n}b = \{\underbrace{b}_{n=0}, \underbrace{a^2b}_{n=1}, \underbrace{ab}_{n=2}\}. \checkmark$$

  This is enough as all remaining elements of D_3 are listed in the conjugacy class of $[b]_C$, thus we do not need to check for rotations in this case. We conclude that the conjugacy classes of D_3 are as follows:

$$[e]_C = \{e\}$$
$$[a]_C = \{a, a^2\}$$
$$[b]_C = \{b, ab, a^2b\}.$$

9.2 Normal subgroups

Definition 9.3. A subgroup H is called **normal** or **invariant** if $gHg^{-1} \subset H$ for all $g \in G$ (equivalently $ghg^{-1} \in H \ \forall h \in H$ and $\forall g \in G$).
If H is a **finite group** then $gHg^{-1} = H$.
If H is normal in G we write $H \triangleleft G$.

Note 9.2. We can interpret a normal subgroup to be a group which under conjugation it remains in itself.

Remark 9.3. The notation $gHg^{-1} = \{ghg^{-1} : h \in H\}$. That is, H is a normal if for every $h \in H$ and every $g \in G$, we have $ghg^{-1} \in H$.

Proposition 9.2

Let $H \subset G$. Properties of normal subgroups:

- If H is normal then $gHg^{-1} = H$ for all $g \in G$.
- The previous property implies $gH = Hg$.
- The group H is normal to G if and only if H is the union of the entire conjugacy classes.
- $\{e\}$ is a (trivial) normal subgroup.
- Every subgroup of an abelian group is normal.
- G and H are normal subgroups of $G \times H$.

Remark 9.4. The last property does not imply that every normal group is abelian.

Example 9.3. Some examples of normal subgroups:

- every subgroup of $\mathbb{Z}_n$ is normal as $\mathbb{Z}_n$ is abelian;
- $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is a normal subgroup of A_4, as $V_4 = [e]_C \cup [(12)(34)]_C \subset A_4$;

Definition 9.4. A group is **simple** if it has no proper normal subgroup(s).

Note 9.3. We can think of simple groups as atomic groups i.e. they cannot be formed by other groups.

Example 9.4. Some examples of groups which are simple or not:

- We have $\mathbb{Z}_p$ for p is a prime are simple groups, while $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$ are not.
- The dihedral groups are not simple groups as $\langle a \rangle \triangleleft D_n$.
- A_5 is a simple group.
- In general the groups A_n with $n > 4$ are all simple groups.

Definition 9.5. A group is **semi-simple** if it has no proper abelian normal subgroup.

Definition 9.6. The **centre** $Z(G)$ of a group G is the set of elements which commute with all elements of G:

$$Z(G) = \{a \in G : ag = ga \ \ \forall g \in G\}.$$

Example 9.5. If G is abelian then $Z(G) = G$.

Theorem 9.1
The centre $Z(G)$ of a group is a normal subgroup.

Proof. We first show that $Z(G)$ is indeed a subgroup.

- Closure: let $a, b \in Z(G)$ and $g \in G$ then $abg = agb = gab$ hence, $ab \in Z(G)$.
- Identity: $e \in Z(G)$.
- Inverse: let $a \in Z(G)$ and $g \in G$ then, $ag^{-1} = g^{-1}a$ hence, $ga^{-1} = a^{-1}g$ which implies $a^{-1} \in Z(G)$.
- Associativity: $Z(G)$ has the same group multiplication rule as G, which is associative as G is a group by construction.

We now prove $Z(G)$ is a normal subgroup. For $a \in Z(G)$ and $g \in G$ we have that $gag^{-1} = gg^{-1}a = a \in Z(G)$. □

Corollary 9.2. Consequently, if G is a finite simple group then $Z(G) = \{e\}$ or $Z(G) = G$.

Proposition 9.3
The centre of the group D_n:

- $Z(D_n) = \{e\}$ for odd n;
- $Z(D_n) = \{e, a^{\frac{n}{2}}\}$ for even n.

Proof. Consider $D_n = \langle a, b \rangle$ with $a^n = e, b^2 = e$ and $a^k b = ba^{-k}$. Elements of $Z(D_n)$ satisfy $zg = gz$ for all $g \in D_n$ and $z \in Z(D_n)$, but we know that

$$a^k b = ba^{-k}.$$

Hence, if any element of the form $a^m \in D_n$ is in $Z(D_n)$ we would require $a^m b = ba^m$; by imposing the condition of D_n we need $a^{-m} = a^m$, for it to commute with b. Now, $a^{-m} = a^m \Rightarrow e = a^{2m}$ but we know that $a^n = e$ thus, the condition becomes $a^n = a^{2m}$. Therefore, if n is odd then a^m is not in the centre whereas, if n is even then $m = \frac{n}{2}$ and $a^{\frac{n}{2}}$ is in the centre. We check the remaining elements of D_n.

- For odd n:

  $$(a^m b)b = ba^{-m}b = b(a^{-m}b)$$

  so, $a^m b$ is not in the centre as $a^m b \neq a^{-m}b$ for odd n.

- For even n:

  $$(a^m b)a = a^m a^{-1} b = a^{-1}(a^m b) = a^{n-1}(a^m b)$$

  and for $n > 2$ we have $a^{-1} \neq a^{n-1}$.

□

9.3 Quotients

Definition 9.7. Let G be a group and H a subgroup of G.

- The **quotient** $G/H = \{gH : g \in G\}$ is the set of all **left-cosets.**
- The **quotient** $H\backslash G = \{Hg : g \in G\}$ is the set of all **right-cosets.**

Definition 9.8. Given two subsets A and B of G, the multiplication of a set A by B is defined by element wise multiplication, $AB := \{ab : a \in A, b \in B\}$.

Theorem 9.2
If H is normal to G then, the quotient G/H with the above multiplication law on subsets is a group.

Note 9.4. The theorem above also applies to right cosets, however we will now focus on left cosets.

Proof. We need to check the axioms of a group.

- Closure: We have $(g_1H)(g_2H) = g_1Hg_2H = g_1(g_2Hg_2^{-1})g_2H = g_1g_2HH = g_1g_2H$, where we have used the fact that H is a normal subgroup of G.
- Associativity: inherent from the associativity of G and the relation above.
- Identity: $e \in H$ is the identity as $eH = H$.
- Inverse: the inverse of gH is $g^{-1}H$ under the multiplication law.

□

10 Kernel and Image of a group

Definition 10.1. Let ϕ be a homomorphism of G onto H (i.e. ϕ is a surjective map to H). Then the **kernel** of ϕ is

$$\ker \phi = \{g \in G : \phi(g) = e_H\}$$

where e_H is the identity element of H.

Remark 10.1. Observe that $e_G \in \ker \phi$.

Example 10.1. Consider the map $\phi : D_3 \to \mathbb{Z}_2$ given by

$$\phi(a^n b^m) = b^m$$

(i.e. $b^m \in \langle b \rangle \cong \mathbb{Z}_2$). This map is indeed a homomorphism as:

$$\phi(a^{n_1}b^{m_1})\phi(a^{n_2}b^{m_2}) = b^{m_1}b^{m_2}$$

while

$$\begin{aligned}\phi(a^{n_1}b^{m_1}a^{n_2}b^{m_2}) &= \phi(a^{n_1}a^{(-1)^{m_1}n_2}b^{m_1}b^{m_2}) \\ &= b^{m_1}b^{m_2} \\ &= \phi(a^{n_1}b^{m_1})\phi(a^{n_2}b^{m_2}).\end{aligned}$$

Then, given $b^m = e$

$$\begin{aligned}\ker\phi &= \{a^nb^m \in D_3 : \phi(a^nb^m) = e \in \mathbb{Z}_2\} \\ &= \{a^nb^m : \forall n \in \mathbb{Z} \text{ and } m \in 2\mathbb{Z}\} \\ &= \{a^n \in D_3 : \forall n \in \mathbb{Z}\} \\ &= \langle a\rangle \\ &\cong \mathbb{Z}_3.\end{aligned}$$

Theorem 10.1

A group homomorphism $\phi : G \to H$ is an isomorphism if and only if it is surjective and $\ker\phi = \{e_G\}$.

Remark 10.2. We can reformulate the theorem above as follows: A group homomorphism $\phi : G \to \operatorname{Im}\phi$ is an isomorphism if and only if $\ker\phi = \{e_G\}$. By the way ϕ has been defined, the surjectivity of ϕ is guaranteed.

Note 10.1. In other words the theorem is saying that a map (of groups) is injective if and only if $\ker\phi = \{e_G\}$.

Theorem 10.2

The kernel is a normal subgroup.

Note 10.2. This is a powerful theorem as it allows us to find a normal subgroup rather simply.

Example 10.2. Let $\phi : D_3 \to \mathbb{Z}_2$ given by $\phi(a^nb^m) = b^m$. We have already shows that this is a homomorphism where we found that $\ker\phi = \langle a\rangle \cong \mathbb{Z}_3$. Therefore, $\mathbb{Z}_3 \cong \langle a\rangle \triangleleft D_3$.

Definition 10.2. Let ϕ be a homomorphism of G on H. Then the **image** of ϕ is

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

Remark 10.3. Notice that for $\phi : G \to H$ we have that $\ker\phi \subset G$ and $\operatorname{Im}\phi \subset H$.

Theorem 10.3

The image $\operatorname{Im}\phi$ of a group homomorphism $\phi : G \to H$ is a subgroup of H.

10.1 The homomorphism theorem

We know that $G/\ker\phi$ is a quotient group since $\ker\phi \triangleleft G$, so the question becomes which group it is.

Theorem 10.4 (The Homomorphism Theorem)
Let G and H be groups and $\phi : G \to H$ be a homomorphism then, $G/\ker\phi \cong \operatorname{Im}\phi$.

Example 10.3. Let $\phi : D_3 \to \mathbb{Z}_2$ given by $\phi(a^n b^m) = b^m$. This is a homomorphism so, by the homomorphism theorem

$$D_3/\mathbb{Z}_3 \cong \mathbb{Z}_2,$$

as $\ker\phi = \langle a\rangle \cong \mathbb{Z}_3$ and $\operatorname{Im}\phi = \langle b\rangle \cong \mathbb{Z}_3$.

Theorem 10.5
Given a group G and a normal subgroup $H \subset G$ then there exists a homomorphism $\phi : G \to G/H$ which is surjective such that $H = \ker\phi$.

Proof. If $g \in G$ define $\phi(g) = gH$. This is a homomorphism:

$$\begin{aligned}\phi(gg') &= gg'H \\ &= gHg'H \\ &= \phi(g)\phi(g').\end{aligned}$$

Its kernel is

$$\begin{aligned}\ker\phi &= \{g \in G : gH = H\} \\ &= \{g \in G : g \sim e\} \\ &= eH \\ &= H.\end{aligned}$$

□

Corollary 10.1. Simple group, having no non-trivial normal subgroup, admit only trivial homomorphism i.e. if $\ker\phi = \{e\}$ then $\operatorname{Im}\phi \cong G$ or, if $\ker\phi = G$ then $\operatorname{Im}\phi = \{e\}$.

11 Automorphism

Definition 11.1. An **automorphism** is an isomorphism of G onto itself.

> **Note 11.1.** An automorphism is a homomorphism $\phi : G \to G$ such that ϕ is surjective.

Definition 11.2. For each element $a \in G$, define the map $\phi_a : G \to G$ by $\phi_a(g) = aga^{-1}$ for all $g \in G$.

- An **inner automorphism** is an automorphism ϕ such that $\phi = \phi_a$ for some $a \in G$.
- If an automorphism ϕ is not inner, then it is called an **outer automorphism**.

> **Note 11.2.** An inner automorphism is an automorphism which admits to a **conjugation** automorphism.

Definition 11.3.
Notation:

- The **set of all automorphism** of a group G is denoted $\mathrm{Aut}(G)$.
- The set of all **inner** automorphism of a group G is denoted $\mathrm{Inn}(G)$.
- The set of all **outer** automorphism of a group G is denoted $\mathrm{Out}(G)$.

Example 11.1. Let $a \in G$ and define $\phi_a : G \to G$ by $\phi_a(g) = aga^{-1}$ for all $g \in G$ (this is the conjugation of g by a). Then ϕ_a is an inner automorphism.

- Homomorphism: $\phi_a(g_1g_2) = ag_1g_2a^{-1} = ag_1\underbrace{a^{-1}a}_{e}g_2a^{-1} = \phi_a(g_1)\phi_a(g_2)$.
- Bijection:
  - Surjective: given $g \in G$ there exists $g' \in G$ such that $\phi_a(g') = g \Rightarrow ag'a^{-1} = g$ therefore, $g' = a^{-1}ga \in G$.
  - Injective: Suppose $\exists g_1 \neq g_2 \in G$ such that $\phi_a(g_1) = \phi_a(g_2)$ then $ag_1a^{-1} = ag_2a^{-1} \Rightarrow g_1 = g_2$ which is a contradiction.

Corollary 11.1. If G is an abelian group then $\mathrm{Inn}(G) = \{\mathrm{id}\}$.

> **Note 11.3.** The identity map being $\phi_a(g) = g$.

Theorem 11.1

The set of all automorphism, $\mathrm{Aut}(G)$, is a group under composition. Furthermore, subset $\mathrm{Inn}(G)$ is a normal subgroup to $\mathrm{Aut}(G)$ i.e. $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

Remark 11.1. $\mathrm{Aut}(G)/\mathrm{Inn}(G) \cong \mathrm{Out}(G)$.

Theorem 11.2
Let G be a group then $G/Z(G) \cong \mathrm{Inn}(G)$.

12 Matrix groups

12.1 Basics

Definition 12.1. The set of all $N \times N$ matrices with elements in $\mathbb{R}$ and $\mathbb{C}$ are denoted by $M_N(\mathbb{R})$ and $M_N(\mathbb{C})$ respectively.

Theorem 12.1 (Matrix operation)**.** We can combine matrices A and B to find another matrix by

- Addition: $A + B = C$ where in components $C_{ij} = A_{ij} + B_{ij}$.
- Matrix multiplication: $AB = C$ where, in components, $C_{ij} = \sum_{k=1}^{N} A_{ik}B_{kj}$.

Note 12.1. The notation for components form, C_{ij}, means the entry on the i^{th} **row** and the j^{th} **column**. So, in matrix multiplication to get the element in the i^{th} row and j^{th} column of the product BA, take the scalar product of the i^{th} row-vector of B with the j^{th} column vector of A.

Definition 12.2. A matrix A is **invertible** if there exists a matrix A^{-1} such that $AA^{-1} = A^{-1}A = I$.

Theorem 12.1

Given any matrix A, we may

- Take its **complex conjugate**, $A^* : (A^*)_{jk} = (A_{jk})^*$.
- Take its **transpose**, $A^\top : (A^\top)_{jk} = A_{kj}$.
- Take its **adjoint**, $A^\dagger = (A^\top)^* = (A^*)^\top$.

Note 12.2. We can interpret the *adjoint* as the **complex-conjugate transpose**.

Definition 12.3. A matrix A is

- **self-adjoint** if $A^\dagger = A$.
- **symmetric** if $A^\top = A$.
- **unitary** if $A^\dagger = A^{-1}$.
- **diagonal** if $A_{jk} = 0$ for all $j \neq k$.

Theorem 12.2

Properties of the determinant:

- $\det(I) = 1$.
- $\det(AB) = \det(A)\det(B)$
- If A^{-1} exists then $\det(A^{-1}) = (\det(A))^{-1} = \frac{1}{\det(A)}$.
- $\det(A) \neq 0$ if and only if A is invertible.
- $\det(A^*) = (\det(A))^*$.
- $\det(A^\top) = \det(A)$.
- $\det(\lambda A) = \lambda^N \det(A)$, where A is an $N \times N$ matrix.
- If A is a diagonal $N \times N$ matrix then $\det(A) = \prod_{j=1}^{N} A_{jj}$, i.e. $\det(A)$ is the product of the diagonal entries.
- $\det(SAS^{-1}) = \det(A)$.
- For an $N \times N$ matrix $\det(\det(A)\mathbb{I}) = (\det(A))^N$.

Proof. We provide a proof of the last property. The matrix $\det(A)\mathbb{I}$ is a diagonal matrix with each diagonal entry being $\det(A)$ therefore, $\det(\det(A)\mathbb{I}) = \det(A)^N$ i.e. the product of the diagonal entries. □

12.2 The classical groups as matrix groups

12.2.1 The General Linear Group

Definition 12.4. The **general linear group** is defined as all $N \times N$ matrices with complex entries and non-zero determinant. It is denoted by

$$\mathrm{GL}(N, \mathbb{C}) = \{A \in M_N(\mathbb{C}) : \det(A) \neq 0\}.$$

Corollary 12.1. The set of $N \times N$ matrices with real entries is a subgroup of $\mathrm{GL}(N, \mathbb{C})$ i.e.

$$\begin{aligned}\mathrm{GL}(N, \mathbb{R}) &= \{A \in M_N(\mathbb{R}) : \det(A) \neq 0\} \\ &\subset \mathrm{GL}(N, \mathbb{C}).\end{aligned}$$

Theorem 12.3

Consider the maps

$$\det : \mathrm{GL}(N, \mathbb{C}) \to \mathbb{C}^* = \mathbb{C}\backslash\{0\} \quad \text{and} \quad \det : \mathrm{GL}(N, \mathbb{R}) \to \mathbb{R}^* = \mathbb{R}\backslash\{0\}$$

are both surjective homomorphisms.

Proof. To show the map is surjective take a diagonal matrix with λ for one of the diagonal entries and the rest of the diagonal to be 1. To show it is a homomorphism use the property of $\det(AB) = \det(A)\det(B)$. □

Theorem 12.4

We have

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

and

$$Z(\mathrm{GL}(N,\mathbb{R})) = \{\lambda\mathbb{I} : \lambda \in \mathbb{R}^*\} \cong \mathbb{R}^*.$$

Remark 12.1. That is the centre of the general linear groups is the set of all diagonal matrices.

12.2.2 The Special Linear Group

Definition 12.5. The **special linear group** is defined as all the $N \times N$ matrices with complex entries and a determinant of 1. It is denoted by

$$\mathrm{SL}(N,\mathbb{C}) = \{A \in M_N(\mathbb{C}) : \det(A) = 1\}.$$

Remark 12.2. The special linear group with real entries is similarly defined and is denoted by $\mathrm{SL}(N,\mathbb{R})$.

Theorem 12.2. The group $\mathrm{SL}(N,\mathbb{R})$ is a normal subgroup of $\mathrm{GL}(N,\mathbb{C})$.

Proof. By definition $\mathrm{SL}(N,\mathbb{C}) = \ker(\det)$, where by " det " we mean the map

$$\det : \mathrm{GL}(N,\mathbb{C}) \to \mathbb{C}^*.$$

□

Theorem 12.3. $\mathrm{GL}(N,\mathbb{C})/\mathrm{SL}(N,\mathbb{C}) \cong \mathbb{C}^*$.

Remark 12.3. Similar theorems are equivalent with real entries.

Theorem 12.5

We have

$$Z(\mathrm{SL}(N,\mathbb{C})) \cong \mathbb{Z}_N$$

and

$$Z(\mathrm{SL}(N,\mathbb{R})) \cong \begin{cases} \mathbb{Z}_2 & \text{if } N \text{ is even} \\ \{\mathbb{I}\} & \text{if } N \text{ is odd.} \end{cases}$$

Remark 12.4. The symbol $\mathbb{I}$ denotes the $N \times N$ identity matrix.

Proof. We outline a proof for each case.

- As before the centres must be matrices proportional to the identity matric i.e. the centre is of the form $\{\lambda\mathbb{I} : \lambda \in \mathbb{C}^*\}$. However, for $A \in \mathrm{SL}(N,\mathbb{C})$ we require $\det(A) = \lambda^N = 1$ which implies that λ must be an N-th root of unity which are isomorphic to $\mathbb{Z}_N$.

- Similarly, we require $\det(A) = \lambda^N = 1$ hence, if N is even we have $\lambda \in \{-1, 1\} \cong \mathbb{Z}_2$ and if N is odd we have $\lambda = 1 \cong \{\mathbb{I}\}$.

□

12.2.3 The Unitary Group

Definition 12.6. The **unitary group** is the group

$$U(N) = \{A \in \mathrm{GL}(N, \mathbb{C}) : A^\dagger = A^{-1}\}$$

where $A^\dagger = (A^*)^\top = (A^\top)^*$.

Note 12.3. We can think of † as the "complex-conjugate transpose".

Proposition 12.1

Some properties of **unitary matrices**, we take $A \in U(N)$:

1. $A^\dagger A = \mathbb{I}$.
2. $|\det(A)| = 1$.
3. $\det(A) = e^{i\theta}$ for some θ.

Corollary 12.2. The group $U(1)$ can be expressed as

$$\begin{aligned} U(1) &= \{z \in \mathbb{C} : zz^* = 1\} \\ &= \{z \in \mathbb{C} : |z| = 1\}. \end{aligned}$$

Note 12.4. The group $U(1)$ parametrises the unit circle, S^1, as $z = e^{i\theta}$.

Theorem 12.6

The map $\det : U(N) \to U(1)$ is a surjective homomorphism.

Proof. To prove surjective let $z \in \mathbb{C}$ with $|z| = 1$ and choose a diagonal matrix with an entry z and the remaining diagonal entries to be 1. □

12.2.4 The Special Unitary Group

Definition 12.7. The **special unitary group** is the group

$$SU(N) = \{A \in U(N) : \det(A) = 1\}.$$

Theorem 12.4. The group $SU(N)$ is a normal subgroup to $U(N)$.

Corollary 12.3. We have

$$U(N)/SU(N) \cong U(1).$$

Proof. Consider the map $\det : U(N) \to U(1)$ with $\ker(\det) = SU(N)$. By the homomorphism theorem we get the isomorphism. □

12.2.5 The Orthogonal Group

Definition 12.8. The **orthogonal group** is the group

$$O(N) = \{A \in M_N(\mathbb{R}) : A^\top = A^{-1}\}.$$

Corollary 12.4. The orthogonal group is a subgroup of the unitary group as $O(N) \subset U(N)$.

Proposition 12.1. If $A \in O(N)$ then $(\det(A))^2 = 1$. If $\det(A) \in \mathbb{R}$ then $\det(A) \in \{-1, 1\} \cong \mathbb{Z}_2$.

Theorem 12.7
The map $\det : O(N) \to \mathbb{Z}_2$ is a surjective homomorphism.

12.2.6 The Special Orthogonal Group

Definition 12.9. The **special orthogonal group** is the group

$$SO(N) = \{A \in O(N) : \det(A) = 1\}.$$

Theorem 12.8
We have that $O(N)/SO(N) \cong \mathbb{Z}_2$.

Proof. Recall $\det : O(N) \to \mathbb{Z}_2$ is surjective also, $\ker(\det) = SO(N)$ hence, by the homomorphism theorem we have that

$$O(N)/SO(N) \cong \mathbb{Z}_2.$$

□

Theorem 12.9
If N is odd then $O(N) \cong \mathbb{Z}_2 \times SO(N)$.

Proof. Consider the map $\phi : O(N) \to \mathbb{Z}_2 \times SO(N)$ given by

$$\phi(A) = \left(\det(A), \frac{A}{\det(A)}\right)$$

for some $A \in O(N)$.
We prove the map is well-defined.

1. $\det(A) \in \mathbb{Z}_2$ as

$$\begin{aligned} A^\top A &= \mathbb{I} \\ \Rightarrow \det(A^\top A) &= 1 \\ \Rightarrow (\det(A))^2 &= 1. \end{aligned}$$

As $\det(A) \in \mathbb{R}$ we must have $\det(A) \in \{-1, 1\} \cong \mathbb{Z}_2$.

2. $\frac{A}{\det(A)} \in O(N)$ as

$$\begin{aligned}\left(\frac{A}{\det(A)}\right)^\top \left(\frac{A}{\det(A)}\right) &= \frac{A^\top A}{(\det(A))^2} \\ &= A^\top A \\ &= \mathbb{I}.\end{aligned}$$

3. $\frac{A}{\det(A)} \in SO(N)$ as

$$\begin{aligned}\det\left(\frac{A}{\det(A)}\right) &= \det(\lambda A) \\ &= \lambda^N \det(A),\end{aligned}$$

where $\lambda = \frac{1}{\det(A)}$. Therefore, we have

$$\begin{aligned}\det\left(\frac{A}{\det(A)}\right) &= \left(\frac{1}{\det(A)}\right)^N \det(A) \\ &= \frac{1}{(\det(A))^{N-1}} \\ &= 1\end{aligned}$$

since N is odd.

We prove surjective:
We can always find a matrix $A \in O(N)$ such that $\phi(A) = (a, B)$. Indeed, just take $A = aB$. This is in $O(N)$ because $A^\top = (aB)^\top = aB^\top$ and $A^{-1} = (aB)^{-1} = a^{-1}B^{-1} = aB^\top$ so, they are both equal (here we have used that $a^{-1} = a$ for $a \in \mathbb{Z}_2$ and $B^{-1} = B^\top$ for $B \in SO(N)$). Also, A has determinant $\det(A) = \det(aB) = a^N \det(B) = a\det(B)$ (since N is odd and $a = \pm 1$), so that $\det(A) = a$ (since $B \in SO(N)$). In conclusion, $\phi(A) = (a, A/a) = (a, B)$, which shows surjectivity. □

12.3 Groups of infinite order

For finite group the order of the group is finite and is defined to be the number of elements in the group.

Definition 12.10. The **real dimension** of a matrix is the number of real numbers needed to specify a particular element in the matrix group.

Remark 12.5. This idea can also be extended to define the **complex dimension**.

Theorem 12.10
$\dim(G/H) = \dim(G) - \dim(H)$.

Theorem 12.5. The real dimension of $\mathrm{GL}(N, \mathbb{R})$ is N^2.

Proof. Each element $A \in \mathrm{GL}(N, \mathbb{R})$ has N^2 real entries subject to the condition that $\det(A) \neq 0$. □

Theorem 12.6. The real dimension of $\mathrm{SL}(N,\mathbb{R})$ is N^2-1.

Proof. Recall that $\frac{\mathrm{GL}(N,\mathbb{R})}{\mathrm{SL}(N,\mathbb{R})} \cong \mathbb{R}^*$ therefore,

$$\begin{aligned}\dim[\mathrm{GL}(N,\mathbb{R})] - \dim[\mathrm{SL}(N,\mathbb{R})] &= \dim(\mathbb{R}^*)\\ N^2 - \dim[\mathrm{SL}(N,\mathbb{R})] &= 1.\end{aligned}$$

This implies that $\dim[\mathrm{SL}(N,\mathbb{R})] = N^2-1$. □

Theorem 12.7. The real dimension of $O(N)$ is $\frac{N(N-1)}{2}$.

Proof. If $A \in O(N)$ then $A \in \mathrm{GL}(N,\mathbb{R})$ so, A has at most N^2 entries. As $A \in O(N)$ then $A^\top A = \mathbb{I}$ but also $\left(A^\top A\right)^\top = \mathbb{I}^\top = \mathbb{I}$. Therefore, we must only consider either upper triangular or lower triangular matrices; each of these matrices has $1+2+\ldots+N = \frac{N(N+1)}{2}$ entries i.e. constraints. The dimension of $O(N)$ is then

$$N^2 - \frac{N(N+1)}{2} = \frac{N(N-1)}{2}.$$

□

Theorem 12.11
The real dimension of $SO(N)$ is $\frac{N(N-1)}{2}$.

Proof. Recall that $\frac{O(N)}{SO(N)} \cong \mathbb{Z}_2$ therefore,

$$\begin{aligned}\dim[O(N)] - \dim[SO(N)] &= \dim(\mathbb{Z}_2)\\ \frac{N(N-1)}{2} - \dim[SO(N)] &= 0.\end{aligned}$$

Which implies that $\dim[SO(N)] = \dim[O(N)] = \frac{N(N-1)}{2}$. □

13 The structure of matrix groups

13.1 $SO(2)$

Let $A \in SO(2)$ be given by $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for $a, b, c, d \in \mathbb{R}$ such that $A^\top A = \mathbb{I}$ and $\det(A) = 1$. Now $A^\top = A^{-1}$ we have that

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \end{aligned}$$

Therefore, $a = d$ and $b = -c$. We can rewrite A as

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ with } \det(A) = a^2 + b^2 = 1.$$

A consistent choice is $a = \cos\theta$ and $b = -\sin\theta$, such that

$$A(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ for } \theta \in [0, 2\pi).$$

By this definition of $A(\theta) \in SO(2)$, we conclude that $SO(2)$ has real dimension 1, as only one parameter is needed to construct a matrix in $SO(2)$. Furthermore, we notice that $SO(2)$ is abelian as by explicit matrix multiplication we have

$$A(\theta)A(\theta') = A(\theta + \theta') \text{ and } A(\theta)^{-1} = A(-\theta).$$

Theorem 13.1
$SO(2) \cong S^1 \cong U(1)$.

Proof. Consider $\phi : SO(2) \to S^1$ given by

$$\phi(A(\theta)) = e^{i\theta} \in S^1.$$

We can also rewrite $U(1) = \{e^{i\theta} : \theta \in [0, 2\pi)\}$. □

Definition 13.1. S^N is the N-dimensional sphere of unit radius i.e.

$$S^N = \left\{ \boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{N+1} \end{pmatrix} \in \mathbb{R}^{N+1} : \|\boldsymbol{x}\| = 1 \right\}$$

Note 13.1. Therefore, $S^1 = \{\boldsymbol{x} \in \mathbb{R}^2 : x^2 + y^2 = 1\}$, which are the set of all points which make up the unit circle. Similarly,

$$S^2 = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1 \right\}.$$

13.2 $SU(2)$

Let $A \in SU(2)$ hence $A^\dagger = A^{-1}$ and $\det(A) = 1$. By applying these defining relations to

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

for $\alpha, \beta, \gamma, \delta \in \mathbb{C}$, we find that

$$\begin{aligned} A^\dagger = \begin{pmatrix} \alpha^* & \gamma^* \\ \beta^* & \delta^* \end{pmatrix} &= \frac{1}{\det(A)} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \\ &= A^{-1} \\ &= \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \end{aligned}.$$

By comparing the entries we find that $\alpha^* = \delta$ and $\gamma^* = -\beta$. Therefore, any matrix $A \in SU(2)$ takes the form

$$A = \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \text{ with } |\alpha|^2 + |\beta|^2 = 1.$$

By writing the complex numbers as

$$\begin{aligned} \alpha &= a + ib_z & \alpha^* &= a - ib_z \\ \beta &= b_y + ib_x & -\beta^* &= -b_y + ib_x, \end{aligned}$$

we find that

$$\begin{aligned} A &= \begin{pmatrix} a + ib_z & b_y + ib_x \\ -b_y + ib_x, & a - ib_z \end{pmatrix} \\ &= a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + ib_x \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + ib_y \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + ib_z \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= a\mathbb{I} + ib_x\sigma_x + ib_y\sigma_y + ib_z\sigma_z \\ &= a\mathbb{I} + i\boldsymbol{b} \cdot \boldsymbol{\sigma}. \end{aligned}$$

Where $\boldsymbol{b} = \begin{pmatrix} b_x \\ b_y \\ b_z \end{pmatrix}$ and $\boldsymbol{\sigma} = \begin{pmatrix} \sigma_x \\ \sigma_y \\ \sigma_z \end{pmatrix}$, so that $\boldsymbol{b} \cdot \boldsymbol{\sigma} = b_x\sigma_x + b_y\sigma_y + b_z\sigma_z$ and also where

$$\sigma_x \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Definition 13.2. The matrices σ_x, σ_y and σ_z are called the **Pauli matrices**.

Theorem 13.1. Each $A \in SU(2)$ is given by a point on $S^3 \subset \mathbb{R}^4$.

Theorem 13.2

The properties of Pauli matrices; this is for any $i \in \{x, y, z\}$.

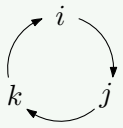
- Traceless, $\mathrm{Tr}(\sigma_i) = 0$.
- Self-adjoint, $\sigma_i^\dagger = \sigma_i$
- $\sigma_i^2 = \mathbb{I}$.
- $\sigma_i \sigma_j = -\sigma_j \sigma_i$ for $i \neq j$.
- $(i\sigma_x)^2 = (i\sigma_y)^2 = (i\sigma_z)^2 = -\mathbb{I}$.

13.2.1 Quaternions

Definition 13.3. The division algebra $\mathbb{H}$ of **quaternions** is the non-commutative algebra of all real linear combinations of i, j, k and $\mathbb{I}$ i.e. $z \in \mathbb{H}$ then $z = a + ib_z + jb_y + kb_x$ where $a, b_x, b_y, b_z \in \mathbb{R}$ with the relations $i^2 = j^2 = k^2 = -1$, $ijk = -1$ and all other cyclic combinations.

Remark 13.1. A **division algebra** is an algebra over which division, except division by zero, is always possible.

Note 13.2. The cyclic combinations of i, j, k can be obtained from the cyclic diagram below:



For example, $ij = k$ as shown by the clockwise orientation of the arrows. Following the anti-clockwise orientation leads to a change in sign, for example $ji = -k$.

Definition 13.4. A **quaternionic conjugate** is defined by:

$$\overline{z} = a - ib_z - jb_y - kb_x.$$

As matrices the conjugate is defined as

$$\overline{z} = z^\dagger.$$

So, $|z| = \sqrt{z\overline{z}}$.

13.2.2 Quaternion group

Definition 13.5. The **Quaternion group** is the group

$$Q_8 = \{1, i, j, k, -i, -j, -k\},$$

where $i^2 = j^2 = k^2 = -1$ and $ijk = -1$.

Note 13.3. Q_8 is equivalent to $\langle a, b\rangle$ with

$$\begin{aligned} a^4 &= e \\ b^2 &= a^2 \\ ab &= -ba. \end{aligned}$$

13.3 Invariant inner product: $O(N)$ and $U(N)$

13.3.1 The inner product

Definition 13.6. Let V be a finite-dimensional vector space over $\mathbb{C}$. A map $V \times V \to \mathbb{C}$ given by $(\boldsymbol{x}, \boldsymbol{y}) \mapsto \langle \boldsymbol{x}, \boldsymbol{y}\rangle$ is an **inner product** if it satisfies:

- $\langle \boldsymbol{x}, \boldsymbol{y}\rangle^* = \langle \boldsymbol{y}, \boldsymbol{x}\rangle$.
- $\langle \boldsymbol{x}, a\boldsymbol{y} + b\boldsymbol{z}\rangle = a\langle \boldsymbol{x}, \boldsymbol{y}\rangle + b\langle \boldsymbol{x}, \boldsymbol{z}\rangle$.
- $\langle \boldsymbol{x}, \boldsymbol{x}\rangle \geq 0$ and if $\langle \boldsymbol{x}, \boldsymbol{x}\rangle = 0$ then $\boldsymbol{x} = 0$.

Corollary 13.1. The first and second property imply

$$\begin{aligned} \langle a\boldsymbol{y} + b\boldsymbol{z}, \boldsymbol{x}\rangle &= \langle \boldsymbol{x}, a\boldsymbol{y} + b\boldsymbol{z}\rangle^* \\ &= (a\langle \boldsymbol{x}, \boldsymbol{y}\rangle + b\langle \boldsymbol{x}, \boldsymbol{z}\rangle)^* \\ &= a^*\langle \boldsymbol{y}, \boldsymbol{x}\rangle + b^*\langle \boldsymbol{z}, \boldsymbol{x}\rangle. \end{aligned}$$

Definition 13.7. An inner product equipped with all the properties above is called **sesquilinear**.

From now on the only inner product we will use is given by

$$\langle \boldsymbol{x}, \boldsymbol{y}\rangle = \sum_i x_i^* y_i = \boldsymbol{x}^\dagger \boldsymbol{y}.$$

Corollary 13.1

For a matrix A we have that

$$\langle \boldsymbol{x}, A\boldsymbol{y}\rangle = \langle A^\dagger \boldsymbol{x}, \boldsymbol{y}\rangle.$$

13.3.2 $O(N)$ and $U(N)$ preserve vector length

Definition 13.8. The **norm** of a vector is defined by

$$\|\boldsymbol{x}\| = \sqrt{\langle \boldsymbol{x}, \boldsymbol{x}\rangle}.$$

Note 13.4. On a Euclidean vector space it is common place to use $\|\boldsymbol{x}\|$ to denote the length of a vector.

Theorem 13.3
A real, linear transformation A of $\mathbb{R}^N$ is such that $\|A\boldsymbol{x}\| = \|\boldsymbol{x}\|$ for all $\boldsymbol{x} \in \mathbb{R}^N$ if and only if $A \in O(N)$.

Note 13.5. The theorem implies that orthogonal transformation preserve vector length.

Theorem 13.4
A complex, linear transformation A of $\mathbb{C}^N$ preserves the norm, $\|A\boldsymbol{x}\| = \|\boldsymbol{x}\|$ for all $\boldsymbol{x} \in \mathbb{C}^N$ if and only if $A \in U(N)$.

13.4 $SO(3)$

Theorem 13.5
If $\boldsymbol{x} \in \mathbb{C}^n$ is an eigenvector of $A \in O(N)$ with eigenvalue λ, then $|\lambda| = 1$.

Theorem 13.2. If $A \in SO(3)$ then there exists a vector $\boldsymbol{n} \in \mathbb{R}^3$ such that $A\boldsymbol{n} = \boldsymbol{n}$.

Proof. Consider $A\boldsymbol{x} = \lambda\boldsymbol{x}$ where $\boldsymbol{x} \in \mathbb{C}^3$, as $A \in SO(3) \subset O(3)$ then $|\lambda| = 1$ by the previous theorem. So, if $(A - \lambda\mathbb{1})\boldsymbol{x} = \boldsymbol{0}$ is non-trivial then $P(\lambda) = \det(A - \lambda\mathbb{1}) = 0$.

$$P(\lambda) = \det \begin{pmatrix} A_{11} - \lambda & A_{12} & A_{13} \\ A_{21} & A_{22} - \lambda & A_{23} \\ A_{31} & A_{32} & A_{33} - \lambda \end{pmatrix},$$

so $P(\lambda)$ is a cubic equation in λ.
Denote the roots of $P(\lambda) = 0$ with $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{C}$. Hence,

$$P(\lambda) = -(\lambda - \lambda_3)(\lambda - \lambda_2)(\lambda - \lambda_1).$$

As $P(0) = 1$ then $P(0) = \lambda_1\lambda_2\lambda_3 = 1$. We need to show that at least one of the λ_1, λ_2 and λ_3 is equal to $+1$. There are two possibilities:

1. If λ_1 is complex but not real, i.e. $\mathrm{Im}(\lambda_1) \neq 0$ then as $|\lambda_1| = 1$ we can write

   $$\lambda_1 = e^{i\alpha}$$

   for $\alpha \in (0, 2\pi)\backslash\{\pi\}$ (so that $\mathrm{Im}(\lambda_1) \neq 0$).
   In this case we have,

   $$A\boldsymbol{x} = \lambda_1\boldsymbol{x} = e^{i\alpha}\boldsymbol{x}.$$

   Since $A \in SO(3)$ and $\lambda_1 \in \mathbb{C}$ we deduce that $\boldsymbol{x}$ is a complex vector. Therefore,

   $$(A\boldsymbol{x})^* = (\lambda_1\boldsymbol{x})^*$$
   $$\Rightarrow A\boldsymbol{x}^* = \lambda_1^*\boldsymbol{x}^* = e^{-i\alpha}\boldsymbol{x}^*.$$

Hence, we have found a second complex eigenvalue, $\lambda_2 = e^{-i\alpha}$. Then as

$$\begin{aligned}\lambda_1\lambda_2\lambda_3 &= 1\\ &= \left(e^{i\alpha}\right)\left(e^{-i\alpha}\right)\lambda_3\\ &= \lambda_3.\end{aligned}$$

So, $\lambda_3 = 1$.

2. All three eigenvalues are real: as $|\lambda_1| = |\lambda_2| = |\lambda_3| = 1$ then

$$\lambda_1, \lambda_2, \lambda_3 \in \{-1, 1\}.$$

As $\lambda_1\lambda_2\lambda_3 = 1$ we can rule out the possibility that $\lambda_1 = \lambda_2 = \lambda_3 = -1$ which implies that at least one of $\lambda_1, \lambda_2, \lambda_3$ must equal to $+1$.

Finally, we show that if $\boldsymbol{x}$ is the **complex eigenvector** with eigenvalue 1 then there exists a **real eigenvector** $\boldsymbol{n}$ with eigenvalue 1. We have $A\boldsymbol{x} = \boldsymbol{x}$ if $\boldsymbol{x} \neq \boldsymbol{x}^*$ then we also have $A\boldsymbol{x}^* = \boldsymbol{x}^*$ so,

$$A(\boldsymbol{x} + \boldsymbol{x}^*) = (\boldsymbol{x} + \boldsymbol{x}^*)$$

then $\boldsymbol{n} = \boldsymbol{x} + \boldsymbol{x}^*$, which is real and has eigenvalue 1. □

Theorem 13.6

Each matrix $A \in SO(3)$ encodes a rotation about an axis spanned by $\hat{\boldsymbol{n}} \in \mathbb{R}^3$.

Note 13.6.

$$SO(3) = \{\text{all rotations about all possible axes in } \mathbb{R}^3\}.$$

Choose a basis of $\mathbb{R}^3$ such that $\hat{\boldsymbol{n}} = \frac{\boldsymbol{n}}{|\boldsymbol{n}|} = \hat{\boldsymbol{e}}_x$ i.e. the unit vector along the x-axis, where $A\boldsymbol{n} = \boldsymbol{n}$ for $A \in SO(3)$. That is

$$\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{31} & A_{33} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

which implies

$$\begin{aligned} A_{11} &= 1\\ A_{21} &= 0\\ A_{31} &= 0.\end{aligned}$$

Further, imposing the properties that A must satisfy to be in $SO(3)$, i.e. $A^\top A = \mathbb{I}$ then we have that A is of the form

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & A_{22} & A_{23} \\ 0 & A_{32} & A_{33} \end{pmatrix}.$$

Denote the 2×2 bottom right matrix by $a = \begin{pmatrix} A_{22} & A_{23} \\ A_{32} & A_{33} \end{pmatrix}$. Then $\det(A) = 1 \Rightarrow \det(a) = 1$ and $A^\top A = \mathbb{I} \Rightarrow a^\top a = \mathbb{I}$ therefore, $a \in SO(2)$. We previously saw the structure matrices in $SO(2)$: rotation matrices,

$$a = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Finally, we have that

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix},$$

hence A is a rotation by θ about the axis spanned by $\hat{\boldsymbol{n}}$.

13.4.1 Geometry of $SO(3)$

Each matrix $A \in SO(3)$ encodes a rotation about an axis spanned by $\hat{\boldsymbol{n}} \in \mathbb{R}^3$. Let $|\boldsymbol{n}| = \theta$ then all the rotations in $\mathbb{R}^3$ (the elements of $SO(3)$) are represented by a ball (of vectors) of radius π where diametrically opposing points of the ball encode the same rotation matrix in $SO(3)$.

13.5 Relating $SU(2)$ to $SO(3)$

Proposition 13.1. There exists a linear bijective map $\Theta : \Sigma \to \mathbb{R}^3$ where Σ is the real, linear space of self-adjoint, traceless 2×2 matrices.

Note 13.7. The Pauli matrices form a basis for Σ.

Proof. Since the Pauli matrices σ_i are a basis for Σ, a general 2×2 matrix can be written in the form $A = a\mathbb{I} + \boldsymbol{b}\cdot\boldsymbol{\sigma}$ for $a, b_x, b_y, b_z \in \mathbb{C}$. The condition of tracelessness imposes $a = 0$ and the condition of self-adjointness imposes $\boldsymbol{b}^* = \boldsymbol{b}$ hence $\boldsymbol{b} \in \mathbb{R}^3$. The space Σ is the space of real linear combinations $A = \boldsymbol{b}\cdot\boldsymbol{\sigma}$. Consider the map Θ given by

$$\Theta(\boldsymbol{b}\cdot\boldsymbol{\sigma}) = \boldsymbol{b},$$

this map is both linear and bijective. □

Theorem 13.7
$SU(2)/\mathbb{Z}_2 \cong SO(3)$.

Proof. Use homomorphism theorem on the surjective map $\varphi : SU(2) \to SO(3)$ with kernel $\ker\varphi \cong \mathbb{Z}_2$. □

14 The Semi-Direct Product

Definition 14.1. A group J is a **semi-direct product** of a subgroup H by a subgroup G if the following conditions are satisfied:

(i) $J = HG$,

(ii) $H \triangleleft J$,

(iii) $H \cap G = \{e\}$ where e is the identity element in J.

The semi-direct product is denoted by $J = G \ltimes H$
(or $J = G \ltimes_\psi H$ where $\psi : G \to \mathrm{Aut}(H)$ given by $\psi(g) = \phi_g$).

Note 14.1. Elements in J, $j \in J$, take the form of $j = hg$ for $h \in H$ and $g \in G$.

Remark 14.1. On the semi-direct product.

1. The **direct product** is a special case of the semi-direct product where both G and H are normal subgroups of J.
2. By the notation $J = G \ltimes H$ we mean that $J \triangleright H$ i.e. H is a normal subgroup of J.
3. Inner product notation: elements of the semi-direct product group are expressed as hg.
4. Outer product notation: elements of the semi-direct product group are expressed as (g, k).

Definition 14.2. The semi-direct product $G \ltimes H$ is the group whose elements are those of the set $G \times H$ and whose multiplication law is

$$(g, h)(g', h') = (gg', h\phi_g(h'))$$

where $\phi_g \in \mathrm{Aut}(H)$.

Theorem 14.1. The multiplication law in the previous equation gives rise to a group structure on the set $G \times H$.

Proof. We check the axioms of a group:

- **Closure**: We have that $gg' \in G$ by closure of G and $\phi_g(h) \in H$ since ϕ_g is an automorphism of H, so that $h\phi_g(h') \in H$ by closure of H.
- **Associativity**:

$$\begin{aligned}
(g_1, h_1)((g_2, h_2)(g_3, h_3)) &= (g_1, h_1)(g_2 g_3, h_2\phi_{g_2}(h_3)) \\
&= (g_1 g_2 g_3, h_1\phi_{g_1}(h_2\phi_{g_2}(h_3))) \\
&= (g_1 g_2 g_3, h_1\phi_{g_1}(h_2)\phi_{g_1}(\phi_{g_2}(h_3))) \\
&= (g_1 g_2 g_3, h_1\phi_{g_1}(h_2)\phi_{g_1 g_2}(h_3)) \\
((g_1, h_1)(g_2, h_2))(g_3, h_3) &= (g_1 g_2, h_1\phi_{g_1}(h_2))(g_3, h_3) \\
&= (g_1 g_2 g_3, h_1\phi_{g_1}(h_2)\phi_{g_1 g_2}(h_3)).
\end{aligned}$$

- **Identity**: The identity element is (e_G, e_H) as:

$$\begin{aligned}(e_G, e_H)(g,h) &= (e_G g, e_H \phi_{e_G}(h)) \\ &= (g,h).\end{aligned}$$

The identity map of $\psi : G \to \mathrm{Aut}(H)$ given by $\psi(g) = \phi_g$ is a homomorphism therefore, $\psi_{e_G} = \phi_{e_G} = \mathrm{id} \in \mathrm{Aut}(H)$.

$$\begin{aligned}(g,h)(e_G, e_H) &= (g e_G, h\phi_g(e_h)) \\ &= (g,h).\end{aligned}$$

Since, $\phi_g : H \to H$ is a homomorphism and so $\phi_g(e_H) = e_H$.

- **Inverse**: The inverse to (g,h) is $(g^{-1}, \phi_{g^{-1}}(h^{-1}))$ as

$$\begin{aligned}(g,h)(g^{-1}, \phi_{g^{-1}}(h^{-1})) &= (gg^{-1}, h\phi_g(\phi_g^{-1})(h^{-1})) \\ &= (gg^{-1}, h\phi_{gg^{-1}}(h^{-1})) \\ &= (e_G, h\phi_{e_G}(h^{-1})) \\ &= (e_G, e_H) \\ (g^{-1}, \phi_{g^{-1}}(h^{-1}))(g,h) &= (g^{-1}g, \phi_{g^{-1}}(h^{-1})\phi_{g^{-1}}(h)) \\ &= (e_G, \phi_{g^{-1}}(h^{-1}h)) \\ &= (e_G, e_H).\end{aligned}$$

□

14.1 $O(N) \cong \mathbb{Z}_2 \ltimes_\psi SO(N)$

Theorem 14.1

$$O(N) \cong \mathbb{Z}_2 \ltimes_\psi SO(N)$$

where the map $\psi : \mathbb{Z}_2 \to \mathrm{Aut}(SO(N))$ is defined by $\psi(s) = \phi_s$ with $\phi_s \in \mathrm{Aut}(SO(N))$ given by $\phi_s(g) = sgs^{-1} = sgs$ for all $s \in \mathbb{Z}_2$ and $g \in SO(N)$.

Proof. We express $\mathbb{Z}_2$ as $N \times N$ matrices such that $\mathbb{Z}_2 = \{\mathbb{I}, R\}$ where $\mathbb{I}$ is the $N \times N$ identity matrix and R is the (reflection) matrix

$$R = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Note $R^2 = \mathbb{I}$ and that $\mathbb{Z}_2 = \{\mathbb{I}, R\}$ is a subgroup of $O(N)$. We show that $\psi : \mathbb{Z}_2 \to \mathrm{Aut}(SO(N))$ given by $\psi(s) = \phi_s$ for $s \in \{\mathbb{I}, R\} \cong \mathbb{Z}_2$ is well-defined. So, we need $\psi \in \mathrm{Aut}(SO(N))$ i.e. ψ is

1. First we show that $\psi : \mathbb{Z}_2 \to \mathrm{Aut}(SO(N))$ given by $\psi(s) = \phi_s$ for $s \in \{\mathbb{I}, R\} \cong \mathbb{Z}_2$ is a well-defined homomorphism i.e. $\psi \in \mathrm{Aut}(SO(N))$.

- ϕ_s is well-defined i.e. $\phi_s(A) \in SO(N)$:
  Consider $\phi_s(A) = sAs$ as $A \in SO(N)$ and $s \in O(N)$ then $sAs \in O(N)$. Next we need $\det(sAs) = 1$. We have,

$$\begin{aligned}\det(sAs) &= \det(s)\det(A)\det(s)\\ &= (\det(s))^2\\ &= 1.\end{aligned}$$

  Therefore, $\det(s) \in \{-1, 1\}$ which implies that $sAs \in SO(N)$.

- ϕ_s is a homomorphism:

$$\begin{aligned}\phi_s(AB) &= sABs\\ &= sAssBs\\ &= \phi_s(A)\phi_s(B).\end{aligned}$$

- ϕ_s is a bijection:
  - Injective: If $\phi_s(A) = \phi_(B)$ then $sAs = sBs$ which implies that $A = B$.
  - Surjective: For any $B \in SO(N)$ we have

$$\phi_s(sBs) = s^2Bs^2 = B,$$

    where $sBs \in SO(N)$.

  Therefore, $\phi_s \in \mathrm{Aut}(SO(N))$.

2. Next, we construct an isomorphism, Φ, that maps $O(N)$ to $\mathbb{Z}_2 \ltimes_\psi SO(N)$.
   We will need a map

$$\omega : O(N) \to \{\mathbb{I}, R\} \cong \mathbb{Z}_2 \quad \text{given by}$$
$$\omega(A) = \begin{cases}\mathbb{I} & \text{if } \det(A) = 1\\ R & \text{if } \det(A) = -1\end{cases}$$

   This map is a homomorphism as for $A, B \in O(N)$ we have

$$\omega(AB) = \begin{cases}\mathbb{I} & \text{if } \det(AB) = 1 \Rightarrow \det(A) = \det(B)\\ R & \text{if } \det(A) \neq \det(B)\end{cases}$$
$$\omega(A)\omega(B) = \begin{cases}\mathbb{I} & \text{if } \det(A) = \det(B)\\ R & \text{if } \det(A) \neq \det(B)\end{cases}$$

   Hence,

$$\omega(AB) = \omega(A)\omega(B).$$

   Using ω we define $\Phi : O(N) \to \mathbb{Z}_2 \ltimes_\psi SO(N)$ given by

$$\Phi(A) = (\omega(A), A\omega(A)) \quad \forall A \in O(N).$$

   We check:

- Φ is well-defined: Notice $\omega(A) \in \{\mathbb{I}, R\} \cong \mathbb{Z}_2$ and $A, \omega(A) \in O(N)$ so, $A\omega(A) \in O(N)$. Furthermore,

$$\begin{aligned}\det(A\omega(A)) &= \det(A)\det(\omega(A)) \\ &= \det(A)\det(\det(A)) \\ &= (\det(A))^2 \\ &= 1.\end{aligned}$$

  Therefore, $A\omega(A) \in SO(N)$.

- Φ is a homomorphism:

$$\begin{aligned}\Phi(A)\Phi(B) &= (\omega(A), A\omega(A))(\omega(B), B\omega(B)) \\ &= (\omega(A), \omega(B), A\omega(A)\phi_{\omega(A)}[B\omega(B)]) \\ &= (\omega(AB), A\omega(A)\omega(A)B\omega(B), \omega(A)) \\ &= (\omega(AB), AB\omega(A)\omega(B)) \\ &= (\omega(AB), AB\omega(AB)) \\ &= \Phi(AB).\end{aligned}$$

  We have used that $\omega(A)\omega(A) = \mathbb{I}$ as $\omega(A) \in \mathbb{Z}_2$ and that $\omega(B)\omega(A) = \omega(A)\omega(B)$ since they are diagonal matrices in $\{\mathbb{I}, R\}$.

- Φ is bijective:
  - Injective: Suppose there exists $A \neq B$ such that $\Phi(A) = \Phi(B)$ then

$$(\omega(A), A\omega(A)) = (\omega(B), B\omega(B)),$$

    which implies $\omega(A) = \omega(B)$ and $A\omega(A) = B\omega(B)$ thus, $A = B$.
  - Surjective: Consider $(s, B) \in \mathbb{Z}_2 \ltimes_\psi SO(N)$ for $s \in \mathbb{Z}_2$ and $B \in SO(N)$ then,

$$\begin{aligned}\Phi(Bs) &= (\omega(Bs), Bs\omega(Bs)) \\ &= (\omega(B)\omega(s), Bs\omega(B)\omega(s)) \\ &= (s, Bs^2) \\ &= (s, B).\end{aligned}$$

    Where we have used the fact that $B \in SO(N)$ so, $\det(B) = 1$ which implies $\omega(B) = \mathbb{I}$, $\omega(s) = s$ and $s \in \mathbb{Z}_2$ so $s^2 = \mathbb{I}$.

□

Theorem 14.2

We have that

- The subset $\{(e, h) : h \in H\} \subset G \times H$ is a subgroup of $G \ltimes_\psi H$ where

$$\{(e, h) : h \in H\} \cong H.$$

  Since, the subgroup is isomorphic to H we have that it is also normal in $G \ltimes_\psi H$.

- The subset $\{(g, e) : g \in G\}$ is a subgroup of $G \ltimes_\psi H$ where

$$\{(g, e) : g \in G\} \cong G.$$

Proof. We prove each statement in turn.

- We show the subset is indeed a subgroup of $G \ltimes H$.
  - Identity: (e, e).
  - Closure: $(e, h)(e, h') = (e, h\phi_e(h')) = (e, hh')$.
  - Inverse: $(e, h)^{-1} = (e, h^{-1})$.

  It is indeed isomorphic to H with $(e, h) \mapsto h$. Furthermore, it is normal as

$$(g, h)^{-1}(e, h')(g, h) = (g^{-1}, \phi_{g^{-1}}(h^{-1}h'))(g, h) = (e, \phi_{g^{-1}}(h^{-1}h'h)).$$

- We prove only closure as the rest is similar to above. Closure: $(g, e)(g, e') = (gg', \phi_g(e)) = (gg', e)$.

□

Theorem 14.3

The left cosets of $G \ltimes H$ with respect to the normal subgroup H are the subsets $\{(g, h) : h \in H\}$. Furthermore,

$$\frac{G \ltimes H}{H} \cong G.$$

Proof. We prove each statement in turn.

- The left cosets are given by $(g, h)(e, H) = (g, h\phi_g(H)) = (g, hH) = (g, H)$.
- The isomorphism is given by $(g, H) \mapsto g$ which is trivially bijective. It is a homomorphism as $(g, H)(g', H) = (gg', H\phi_g(H)) = (gg', H)$.

□

15 The Euclidean Group

The Euclidean group is the group of all transformation of $\mathbb{R}^N$ that leave the distance

$$D(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\| = \sqrt{\langle \boldsymbol{x} - \boldsymbol{y}, \boldsymbol{x} - \boldsymbol{y} \rangle}$$

between any two points $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^N$ invariant.

Proposition 15.1. $(\mathbb{R}^N, +)$ is an abelian group.

Theorem 15.1
The set of all translations of $\mathbb{R}^N$ forms a group which is isomorphic to $\mathbb{R}^N$.

Proof. Let $T_{\boldsymbol{b}} : \mathbb{R}^N \to \mathbb{R}^N$ be given by $T_{\boldsymbol{b}} = \boldsymbol{x} + \boldsymbol{b}$. So, $T_{\boldsymbol{b}}$ is a translation by $\boldsymbol{b} \in \mathbb{R}^N$. We check the axioms of groups:

- Closure: $T_{\boldsymbol{b}} \circ T_{\boldsymbol{c}} = T_{\boldsymbol{b}}(T_{\boldsymbol{c}}(\boldsymbol{x})) = T_{\boldsymbol{b}+\boldsymbol{c}}$ for all $\boldsymbol{x} \in \mathbb{R}^N$.
- Associativity: inherent from the composition of maps.
- Identity: Translation by $\mathbf{0}$ is the identity i.e. $T_{\mathbf{0}}$.
- Inverse: $T_{-\boldsymbol{b}}$ is the inverse to $T_{\boldsymbol{b}}$ as $T_{-\boldsymbol{b}} \circ T_{\boldsymbol{b}} = T_{\mathbf{0}} = T_{\boldsymbol{b}} \circ T_{-\boldsymbol{b}}$.

Hence, the set of all translations is a group.
Consider the map $\phi(T_{\boldsymbol{b}}) = \boldsymbol{b}$, a map from the translation group to $\mathbb{R}^N$. This is a homomorphism as

$$\begin{aligned} \phi(T_{\boldsymbol{b}} \circ T_{\boldsymbol{c}}) &= \phi(T_{\boldsymbol{b}+\boldsymbol{c}}) \\ &= \boldsymbol{b} + \boldsymbol{c} \\ &= \phi(\boldsymbol{b}) + \phi(\boldsymbol{c}). \end{aligned}$$

It is also bijective by construction therefore, $\mathbb{R}^N$ under addition is isomorphic to the group of translations. □

Theorem 15.2
The set of transformation $Q : \mathbb{R}^N \to \mathbb{R}^N$ such that $D(Q(\boldsymbol{x}), Q(\boldsymbol{y})) = D(\boldsymbol{x}, \boldsymbol{y})$ consists of combinations of translations and orthogonal transformations.

Note 15.1. The theorem is saying that all length preserving transformations on $\mathbb{R}^N$ consists **only** of translations and orthogonal transformations.

Definition 15.1. The **Euclidean group** is

$$E_N = O(N) \ltimes_{\psi} \mathbb{R}^N$$

where $\psi : O(N) \to \mathrm{Aut}(\mathbb{R}^N)$ given by $\psi(A) = \varphi_A$ is a homomorphism, with φ_A defined by

$$\varphi_A(\boldsymbol{b}) = A\boldsymbol{b}$$

where $A \in O(N)$ and $\boldsymbol{b} \in \mathbb{R}^N$.

Proof. We need to check: the Euclidean group is well-defined, ψ being a homomorphism and φ is an automorphism.

1. φ is an automorphism.
   If φ_A is bijective then it has an inverse. Since $A^{-1} \in O(N)$ we have that $\varphi_{A^{-1}}$ is the inverse to the map φ_A as

   $$\varphi_{A^{-1}} \circ \varphi_A(\boldsymbol{b}) = A^{-1}A\boldsymbol{b} = \boldsymbol{b}$$

   and $\varphi_{A^{-1}} \circ \varphi_A(\boldsymbol{b}) = \boldsymbol{b}$.
   φ_A is a homomorphism.

   $$\begin{aligned}\varphi_A(\boldsymbol{b}+\boldsymbol{x}) &= A(\boldsymbol{b}+\boldsymbol{x})\\ &= A\boldsymbol{b} + A\boldsymbol{c}\\ &= \varphi_A(\boldsymbol{b}) + \varphi_A(\boldsymbol{c}).\end{aligned}$$

2. ψ is a homomorphism.

   $$\begin{aligned}\psi(AB)(\boldsymbol{b}) &= \varphi_{AB}(\boldsymbol{b})\\ &= AB(\boldsymbol{b})\\ &= \varphi_A \circ \varphi_B(\boldsymbol{b})\\ &= (\psi(A)\psi(B))(\boldsymbol{b})\end{aligned}$$

   for all $\boldsymbol{b} \in \mathbb{R}^N$.

3. The Euclidean group is well-defined.
   By checking the properties above we have shown that the Euclidean group is well-defined.

□

A general element of the Euclidean group will consist of both an orthogonal transformation and translation which we will denote as $(A, T_{\boldsymbol{b}}) = T_{\boldsymbol{b}} \circ A$ (the LHS is in outer product notation and the RHS is in the inner product notation).

$$(A, T_{\boldsymbol{b}})(\boldsymbol{x}) = T_{\boldsymbol{b}}(A(\boldsymbol{x})) = A\boldsymbol{x} + \boldsymbol{b}.$$

Theorem 15.1. The multiplication rule of the semi-direct product of the Euclidean group is defined as

$$(A, \boldsymbol{b})(A', \boldsymbol{b}') = (AA', \boldsymbol{b} \cdot (\phi_A(\boldsymbol{b}'))) = (AA', A\boldsymbol{b}' + \boldsymbol{b}),$$

where $\phi_A = A\boldsymbol{b}$.

Theorem 15.3
The Euclidean group, E_N, is the group generated by translations and orthogonal transformations of $\mathbb{R}^N$.

16 G-sets, stabilisers and orbits

Definition 16.1. For a group G a **G-set** is a set X equipped with a rule assigning to each element $g \in G$ and each element $x \in X$ an element $g \cdot x \in X$ satisfying:

(i) $e \cdot x = x$ for all $x \in X$ where $e \in G$ is the identity element of G;

(ii) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $g_1, g_2 \in G$ and $x \in X$.

Definition 16.2. Given a G-set, X, the **stabiliser**, G_x, of $x \in X$ is the set of elements $g \in G$ such that $g \cdot x = x$ i.e.

$$G_x = \{g \in G : g \cdot x = x\}.$$

Theorem 16.1
G_x is a subgroup of G.

Definition 16.3. When $X = G$ and the G-set action is $g \cdot x = gxg^{-1}$ then G_x is called the **centraliser** of an element x and denoted:

$$\begin{aligned} C_G(x) &= \{g \in G : gxg^{-1} = x\} \\ &= \{g \in G : gx = xg\}. \end{aligned}$$

Remark 16.1. The centre, $Z(G)$, consists of all those elements in G which commute with **all** other of G. Whereas, $C_G(x)$ consists of all elements of G which commute with a **single element** $x \in G$.

Example 16.1
The centraliser of $b \in D_3$:

$$C_{D_3}(b) = \{g \in D_3 : gbg^{-1} = b\}.$$

As the centraliser is a subgroup of D_3 it has order $1, 2, 3$ or 6. Since, D_3 is not abelian then $|C_{D_3}| \neq 6$. The subgroup $\langle b \rangle \subset C_{D_3}(b)$; since $\langle b \rangle$ is a subgroup of $C_{D_3}(b)$ by Lagrange's theorem $|\langle b \rangle|$ divides $|C_{D_3}(b)|$. So, as $|\langle b \rangle| = 2$ then $|C_{D_3}(b)| = 2$. Hence, $C_{D_3} = \langle b \rangle = \{e, b\}$.

Definition 16.4. When X is the set of subgroups in G with action $g \cdot H = gHg^{-1}$ where $H \in X$ is a subgroup of G then the stabiliser, G_H, is called the **normaliser**. It is denoted by

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

Theorem 16.1. The normaliser, $N_G(H)$ is a subgroup of G that always contains H.

Example 16.1. The normaliser of $\langle b \rangle \subset D_3$ is:

$$N_{D_3}(\langle b \rangle) = \{g \in D_3 : g\langle b \rangle g^{-1} = \langle b \rangle\}.$$

Now $\langle b\rangle \subset N_{D_3}(\langle b\rangle)$ and $|\langle b\rangle| = 2$ so $|N_{D_3}(\langle b\rangle)| = 2$ or 6 (by Lagrange's theorem). If the normaliser has order 6 then it must contain all of D_3, but this is not the case as if $g = a$ we find that

$$\begin{aligned} a\langle b\rangle a^{-1} &= a\{e, b\}a^{-1} \\ &= \{aea^{-1}, aba^{-1}\} \\ &= \{e, a^2b\} \\ &\neq \langle b\rangle. \end{aligned}$$

So, $a \notin N_{D_3}(\langle b\rangle)$ hence, $|N_{D_3}(\langle b\rangle)| = 2$. Therefore, $N_{D_3}(\langle b\rangle) = \langle b\rangle = \{e, b\}$.

Remark 16.2. This is the same as observing that $\langle b\rangle$ is **not** a normal subgroup. On the other hand $a \triangleleft D_3$ so, $N_{D_3}(\langle a\rangle) = D_3$.

Definition 16.5. The **orbit** of x in a G-set, X, is given by

$$\text{orb}(x) = \{g \cdot x : \forall g \in G\}.$$

Theorem 16.2

The orbit of an element, $x \in X$, is an equivalence class with equivalence relation $y \sim x$ if there exists a $g \in G$ such that $y = g \cdot x$.

Corollary 16.1. Orbits partition the G-set i.e.

$$|X| = |\text{orb}(x_1)| + |\text{orb}(x_2)| + \cdots + |\text{orb}(x_n)|\,,$$

where $x_1, x_2, \ldots, x_n$ are representative elements from each of the distinct orbits that cover X.

Proof. As equivalence classes are either or identical or disjoint then the orbits partition X. □

Example 16.2. If $X = G$ and $g \cdot x = gx$ then $\text{orb}(x) = G$ (while the stabiliser $G_x = \{e\}$).

Example 16.2

If X is the set of all left cosets of G with respect to a subgroup $H \subset G$ with group action $g \cdot (g_1H) = gg_1H$. Then $\text{orb}(H)$ is the set of all left cosets of H in G. (While the stabiliser $G_H = H$).

Example 16.3. For $X = G$ with $g \cdot x = gxg^{-1}$ then $\text{orb}(x)$ is the conjugacy class of x.

Theorem 16.3 (Orbit-stabiliser theorem)

Let G be a finite group and X be a G-set. For each $x \in X$

$$|\text{orb}(x)| = \frac{|G|}{|G_x|}.$$

Proof. We will construct a bijection between the elements of $\text{orb}(x)$ and the cosets $gG_x \in G/G_x$ given by

$$M(g \cdot x) = gG_x.$$

- Injective: suppose $\exists g, h \in G$ such that $g \cdot x \neq h \cdot x$ but $M(g \cdot x) = M(h \cdot x)$. So,

$$\begin{aligned} gG_x &= hG_x \\ \Rightarrow h^{-1}gG_x &= G_x \\ \Rightarrow h^{-1}g &\in G_x. \end{aligned}$$

  Therefore, $(h^{-1}g) \cdot x = x$ which implies $g \cdot x = h \cdot x$ which contradicts the assumption that $g \cdot x \neq h \cdot x$.

- Surjective: by construction, i.e. the pre-image $gG_x \in G/G_x$ is $g \cdot x \in \text{orb}(x)$.

Hence, M is bijective, which means $|\text{orb}(x)| = |G/G_x| = \frac{|G|}{|G_x|}$. □

Example 16.3

Consider $G = D_3$:

- When $x = e$, $C_{D_3}(e) = \{g \in D_3 : geg^{-1} = e\} = D_3$ so,

$$|\text{orb}(e)| = \frac{|D_3|}{|C_{D_3}(e)|} = \frac{|D_3|}{|D_3|} = 1.$$

- When $x = a$, we know that $\langle a \rangle \subset C_{D_3}(a)$ then as $|\langle a \rangle| = 3$ we have that $|C_{D_3}|(a) = 3$ or 6. It cannot be 6 as $a \notin Z(D_3)$. Therefore, $|C_{D_3}| = 3$ which implies $|\text{orb}(a)| = \frac{6}{3} = 2$ so, $\text{orb}(a) = \{a, a^2\}$.

- When $x = b$ then $\langle b \rangle C_{D_3}(b)$ so $|C_{D_3}(b)| = 2$ hence, $|\text{orb}(b)| = \frac{6}{2} = 3$ which implies $\text{orb}(b) = \{b, ab, a^2b\}$.

Example 16.4. Let X be the set of any permutation of all the letters of the word BANANAS. How many distinct 'words' are there in X.
Solution: The symmetric group S_7 acts on the letter to give all permutations, $|S_7| = 7!$. So,

$$|\text{orb(BANANAS)}| = \frac{|S_7|}{3! \cdot 2!}.$$

Where, 3! represents the permutation of the 3 A's and 2! the permutation of the 2 N's.

Theorem 16.4

Let G be a finite group of order p^n where p is prime and $n \in \mathbb{Z}^+$. Then $Z(G)$ contains more than one element.

Proof. Let $X = G$ with $g \cdot x = gxg^{-1}$. As the conjugacy classes cover G then

$$|G| = |\text{orb}(g_1)| + |\text{orb}(g_2)| + \ldots + |\text{orb}(g_k)|.$$

At least one of the conjugacy classes is that of the identity element thus, it contains just a single element, i.e. $|\operatorname{orb} e| = 1$ so,

$$|G| = 1 + |\operatorname{orb}(g_1)| + |\operatorname{orb}(g_2)| + \ldots + |\operatorname{orb}(g_{k-1})|\,.$$

As $|G| = p^n$ then by the orbit-stabiliser theorem we have that

$$|\operatorname{orb} g_i| = \frac{|G|}{|C_G(g_i)|} = \frac{p^n}{p^{m_i}} = p^{n-m_i}$$

for some integer $m_i \leq n$ and for each $\operatorname{orb}(g_i)$. Therefore,

$$|G| = 1 + p^{m_1} + p^{m_2} + \ldots p^{m_{k-1}}.$$

Since, $|G| = p^n$ we must have that $|G| \equiv 0 \pmod p$ whereas, the RHS $\equiv 1 \pmod p$. Therefore, at least one or more conjugacy class must contain only one element. Suppose $\operatorname{orb}(g_1) = \{g_1\}$ then $m_1 = 0$ and $gg_1g^{-1} = g$ for all $g \in G$, this implies $gg_1 = g_1g$ for all $g \in G$ hence, $g_1 \in Z(G)$ with e so $|Z(G)| > 1$. □

Theorem 16.2. Let G be a group such that $G/Z(G)$ is a cyclic group. Then G is abelian so, $Z(G) = G$.

Proof. Suppose that $\frac{G}{Z(G)}$ is a cylic group generated by $gZ(G)$ hence, every element of G lies in one of the cosets $g^nZ(G)$ for $n \in \mathbb{Z}$. Therefore, any pair of elements $g_1, g_2 \in G$ may be written as $g_1 = g^{n_1}z_1$ and $g_2 = g^{n_2}z_2$. Now,

$$g_1g_2 = g^{n_1}z_1g^{n_2}z_2 = g^{n_1}g^{n_2}z_1z_2 = g^{n_1+n_2}z_2z_1 = g^{n_2}z_2g^{n_1}z_1 = g_2g_1.$$

Therefore, G is abelian. □

Theorem 16.5

Any finite group with $|G| = p^2$ elements, where p is prime, is abelian.

Proof. As $|G| = p^2$ then $|Z(G)| > 1$. Since $Z(G)$ is a subgroup then $|Z(G)|$ is p or p^2. If $|Z(G)| = p^2$ then $Z(G) = G$ and G is abelian. If $|Z(G)| = p$ then, $\left|\frac{G}{Z(G)}\right| = p$ which implies $\frac{G}{Z(G)}$ is isomorphic to a cyclic group hence, G is abelian and this implies $Z(G) = G$, which is a contradiction. So, $|Z(G)| = p$ is not allowed. □

Lemma 16.1

Let G and H be two subgroups of a finite group J. Then

$$|J| = |GH| = \frac{|G|\,|H|}{|G \cap H|}.$$

Theorem 16.6
A group of order p^2 is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$, where p is prime.

Proof. The order of each element in G must divide $|G| = p^2$. Hence, each element $g \in G$ has order $1, p$ or p^2. If G contains an element of order p^2 then $G \cong \mathbb{Z}_{p^2}$. If G has only (non-identity) elements of order p, then let g and h be two such elements such that $\langle g \rangle \cap \langle h \rangle = \{e\}$. Then using the lemma above

$$|\langle g \rangle \langle h \rangle| = \frac{|\langle g \rangle|\,|\langle h \rangle|}{|\langle g \rangle \cap \langle h \rangle|} = \frac{p^2}{1} = p^2.$$

Hence, $\langle g \rangle \langle h \rangle$ covers G and the distinct elements of G take the form $g^n h^m$ for $0 \leq n, m < p - 1$. Using $\phi(g^n h^m) = (g^n, h^m) \in \mathbb{Z}_p \times \mathbb{Z}_p$ we can show that

$$\langle g \rangle \langle h \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

□

Remark 16.3. Notice $\mathbb{Z}_{p^2}$ is cyclic whereas $\mathbb{Z}_p \times \mathbb{Z}_p$ is not cyclic.

Remark 16.4. Hence, there are only two groups (up to isomorphism) of order $4, 9, 15, 25, \ldots$ both of which are abelian.

17 The Sylow theorems

Definition 17.1. Let p be a positive, prime integer. A **p-group** is a group in which every element has order of a power of p.

Remark 17.1. If G is a finite p-group, then $|G| = p^k$ for some k.

Example 17.1. $\mathbb{Z}_p$ for a prime p is a p-group. Whereas $|D_3| = 6 = 2 \cdot 3$ is not a p-group as its order is not some power of a prime p.

Definition 17.2. A **p-subgroup** is one in which every element is a power of p.

Remark 17.2. A p-subgroup does not necessarily need to be a subgroup of a p-group.

Definition 17.3. Let G be a finite group with $|G| = mp^k$ where p is a prime which *does not* divide $m \in \mathbb{Z}$ i.e. $p \nmid m$. A subgroup of order p^k is called a **Sylow p-subgroup**.

Remark 17.3. A Sylow p-subgroup is the maximal p-subgroup in G.

Example 17.1

Let $|G| = 60 = 2^2 \cdot 3 \cdot 5$ then, potentially G may have:

- Sylow 2-subgroup of order $2^2 = 4$,
- Sylow 3-subgroup of order 3 and
- Sylow 5-subgroup of order 5.

The Sylow theorems tells us that these Sylow p-subgroup exists and how many there are.

Theorem 17.1 (Sylow theorems)

Let G be a (finite) group of order mp^k where p is prime and $p \nmid m$, then:

I. a Sylow p-subgroup exists,

II. for each prime p, the Sylow p-subgroup are conjugate to each other and

III. Let n_p be the number of Sylow p-subgroups then

(i). $n_p \equiv 1 \pmod{p}$,

(ii). $n_p = \frac{|G|}{|N_G(P)|}$ where $N_G(P)$ is the normaliser of the Sylow p-subgroup $P \subset G$ and

(iii) $n_p \mid m$ (n_p is the index of the Sylow p-subgroup in G).

Remark 17.4. Sylow II: suppose there exists multiple Sylow 5-subgroup then, each of the subgroups are conjuagte to each other.

Example 17.2

For $G = D_3$, as $|D_3| = 6 = 2 \cdot 3$ then:

- for $p = 2$ then $m = 3$ hence, Sylow (I) implies a 2-subgroup of order 2 exists i.e. $\langle b \rangle \cong \mathbb{Z}_2$.
  - Sylow (III) implies by
    (i). $n_2 \equiv 1 \pmod 2$, so $n_2 = 1, 3, 5 \ldots$
    (ii). $n_2 \leq |D_3| = 6$
    (iii). n_2 divides 3 which implies $n_2 = 1$ or 3.
    For example, let $P = \langle b \rangle$ then $P \subset N_{D_3}(P)$ so, $|N_{D_3}(P)| = 2$ or 6. P is not a normal subgroup so $n_2 = \frac{|D_3|}{|N_{D_3}(P)|} = \frac{6}{2} = 3$.
  - Sylow (II) implies these subgroups are $\langle b \rangle, \langle ab \rangle$ and $\langle a^2 b \rangle$ obtained by conjugation as $a\langle b \rangle a^{-1} = \langle a^2 b \rangle$ and $a\langle a^2 b \rangle a^{-1} = \langle ab \rangle$.
- For $p = 3$ then $m = 2$:
  - Sylow (I) implies a 3-subgroup of order 3 exists.
  - Sylow (III)
    (i). $n_3 \equiv 1 \pmod 3$ so, $n_3 = 1$ or 4.
    (ii). $n_3 \leq 6$.
    (iii). n_3 divides 2 so $n_3 = 1$.
    The Sylow 3-subgroup is $\langle a \rangle$.
  - Sylow (II) implies $a\langle a \rangle a^{-1} = \langle a \rangle$ and $b\langle a \rangle b^{-1} = \langle a^2 \rangle = \langle a \rangle$. Conjugation does not produce any new 3-subgroups. Hence, $\langle a \rangle$ is a normal subgroup.

Theorem 17.2

A Sylow p-subgroup is a normal subgroup if and only if it is the only Sylow p-subgroup i.e. $n_p = 1$.

Proof. We will prove it in two parts.

- Proof of ($\Rightarrow$). If $P \triangleleft G$ then $gPg^{-1} = P$ hence there are no new conjugate subgroups which implies $n_p = 1$.
- Proof of ($\Leftarrow$). If $n_p = 1$ then $gPg^{-1} = P$ therefore, $P \triangleleft G$.

□

17.1 Example use of the Sylow theorems

Example.

Any group of order 6 must have a Sylow 2-subgroup P and a Sylow 3-subgroup Q.

Now $n_3 = 1, 4, \ldots$ and n_3 divides 2 so $n_3 = 1$ $\therefore Q \triangleleft G$, and $Q \cong \mathbb{Z}_3 = \langle y \rangle$ with $y^3 = e$. While $n_2 = 1, 3, 5 \ldots$ and n_2 divides 3 so $n_2 = 1$ or 3. Let $P = \langle x \rangle$ with $x^2 = e$, so $P \cong \mathbb{Z}_2$. As $Q \triangleleft G$ we have $xyx^{-1} \in Q = \{e, y, y^2\}$:

- if $xyx^{-1} = e$ then $y = e$ which is inconsistent and so not possible,
- if $xyx^{-1} = y$ then $xy = yx$ (so G is abelian) and

$$\langle xy \rangle = \{xy,\ xyxy,\ xyy^2,\ xxy,\ yxy,\ xy^2xy\}$$

$$= \{xy,\ y^2,\ x,\ y,\ xy^2,\ e\}$$

so $xy \in G$ is an element of order 6 $\therefore$ $G = \mathbb{Z}_6$.

- if $xyx^{-1} = y^2 = y^{-1}$ then $xy = y^{-1}x$ with $x^2 = e$, $y^3 = e$ $\therefore \langle x, y \rangle = D_3$.

Example

All groups of order 15 are cyclic groups:

As $|G| = 15 = 3 \cdot 5$ then G has a Sylow 3-subgroup P and a Sylow 5-subgroup Q.

Now $n_3 = 1 \bmod 3 = 1, 4, 7, 10, 13\ldots$; n_3 divides 5 $\Rightarrow n_3 = 1$. $\therefore P \triangleleft G$.

Also $n_5 = 1 \bmod 5 = 1, 6, 11$; n_5 divides 3 $\Rightarrow n_5 = 1$ $\therefore Q \triangleleft G$.

So G contains 1 element of order 1 (e), 2 elements of order 3 in P, 4 elements of order 5 in Q. This accounts for $1 + 2 + 4 = 7$ elements of G, the remaining 8 elements must all have order 15 as every element of G must have order 1, 3, 5 or 15 and because $n_3 = 1$, $n_5 = 1$ we have accounted for all those elements of orders 1, 3 or 5. $\therefore G = \mathbb{Z}_{15}$

i.e. if $\mathbb{Z}_{15} = \langle a \rangle$ with $a^{15} = e$ then

$$\mathbb{Z}_{15} = \{ e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{13}, a^{14} \}$$

orders: 1, 15, 15, 5, 15, 3, 5, 15, 15, 5, 3, 15, 5, 15, 15.

Example.

$|D_5| = 10 = 2 \cdot 5$

It has a Sylow 2-subgroup P with $n_2 = 1, 3, 5, 7, 9$, n_2 divides 5

$\Rightarrow n_2 = 1$ or 5

as $a\langle b\rangle a^{-1} = \langle a^2 b\rangle \neq \langle b\rangle$

then $n_2 = 5$

Now $P_c = \{ g\langle b\rangle g^{-1} \mid g \in G \}$

$= \{ \langle b\rangle, \langle a^2 b\rangle, \langle a^4 b\rangle, \langle ab\rangle, \langle a^3 b\rangle \}$

$\therefore$ all 5 Sylow 2-subgroups are conjugate to each other.

Under conjugation with elements of $P = \langle b\rangle$ we find the P-orbits:

$orb(\langle b\rangle) = \{\langle b\rangle\}$ $\quad \therefore |orb(\langle b\rangle)| = 1 = 2^0$

$orb(\langle a^2 b\rangle) = \{\langle a^2 b\rangle, \langle a^3 b\rangle\}$ $\quad |orb(\langle a^2 b\rangle)| = 2 = 2^1$

$orb(\langle a^4 b\rangle) = \{\langle a^4 b\rangle, \langle ab\rangle\}$ $\quad |orb(\langle a^4 b\rangle)| = 2 = 2^1$

N.B. $|P_c| = 1 \bmod p$ indeed $|P_c| = 5$.

D_5 also has a Sylow 5-subgroup with $n_5 = 1$ or 6; n_5 divides 2 $\therefore n_5 = 1$

hence $\langle a\rangle \cong \mathbb{Z}_5 \subset D_5$ is a normal subgroup.

Example

Find all groups of order 21.

$21 = 3 \cdot 7$ $\Rightarrow$ $\exists$ a Sylow 3-subgroup, P and $|P| = 3$ $\quad P \cong \mathbb{Z}_3$.

$\Rightarrow$ $\exists$ a Sylow 7-subgroup, Q and $|Q| = 7$ $\quad Q \cong \mathbb{Z}_7$

$n_3 = 1 \bmod 3 = 1, 4, 7, \ldots$ $\quad n_3$ must be a factor of 7 so $n_3 = 1$ or 7

$n_7 = 1 \bmod 7 = 1, 8, \ldots$ $\quad n_7$ must be a factor of 3 so $n_7 = 1$.

$\therefore \mathbb{Z}_7 \cong Q \triangleleft G$ where $|G| = 21$.

Let $P = \langle x \rangle$ with $x^3 = e$ and $Q = \langle y \rangle$ with $y^7 = e$.

As $Q \triangleleft G$ and $P \subset G$ then $xyx^{-1} \in Q = \{e, y, y^2, y^3, y^4, y^5, y^6\}$.

Suppose we write $xyx^{-1} = y^n$ where $n = \{0, 1, 2, 3, 4, 5, 6\}$.

Then,

$$y = x^3 y x^{-3} \qquad \text{as } x^3 = e, \text{ so } x^{-3} = e.$$

$$= x^2 (xyx^{-1}) x^{-2}$$

$$= x^2 y^n x^{-2}$$

$$= x (x y^n x^{-1}) x^{-1} \qquad \text{as } (xyx^{-1})^n = (xyx^{-1})(xyx^{-1}) \ldots (xyx^{-1}) = x y^n x^{-1}.$$

$$= x (xyx^{-1})^n x^{-1} \qquad (xyx^{-1} \text{ underbrace } y^n)$$

$$= x y^{n^2} x^{-1}$$

$$y = y^{n^3}. \qquad \text{where } n \in \{0, 1, 2, 3, 4, 5, 6\}.$$

$x^3 = e$, $y^7 = e$, $xyx^{-1} = y^n$ $n \in \{0, 1, \dots, 6\}$ and $y = y^{n^3}$.

If $y = y^{n^3}$ then $n^3 = 1 \bmod 7$.

$0^3 = 0 \bmod 7$ ×, $1^3 = 1 \bmod 7$ ✓, $2^3 = 1 \bmod 7$ ✓

$3^3 = (3 \cdot 9) \bmod 7 = (3 \cdot 2) \bmod 7 = 6 \bmod 7$ ×

$4^3 = 1 \bmod 7$ ✓, $5^3 = 6 \bmod 7$ ×, and $6^3 = 6 \bmod 7$. ×

Only 3 possibilities remain as $n = 1$, 2 or 4.

⇒ 3 possible groups each one is $\langle x, y \rangle$ with $x^3 = e$, $y^7 = e$ and :

- G_1 has (in addition) $xyx^{-1} = y$ ⇒ $xy = yx$ and $|\langle xy \rangle| = 21$

$\therefore G_1 \cong \mathbb{Z}_{21}$.

- G_2 has (in addition) $xyx^{-1} = y^2$

- G_4 has (in addition) $xyx^{-1} = y^4$

N.B. G_2 and G_4 are isomorphic : In G_2 consider $x^2 y x^{-2} = x y^2 x^{-1} = (xyx^{-1})^2 = y^4$.

So if we relabel G_2 elements by defining $z = x^2$ then

$G_2 = \langle z, y \rangle$ with $z^3 = e$, $y^7 = e$ and $zyz^{-1} = y^4$.

So $G_2 \cong G_4$.

Example.

$|D_5| = 10 = 2 \cdot 5$

It has a Sylow 2-subgroup P with $n_2 = 1, 3, 5, 7, 9$, n_2 divides 5

$\Rightarrow n_2 = 1$ or 5

as $a\langle b\rangle a^{-1} = \langle a^2 b\rangle \neq \langle b\rangle$

then $n_2 = 5$

Now $P_c = \{ g\langle b\rangle g^{-1} \mid g \in G \}$

$= \{ \langle b\rangle, \langle a^2 b\rangle, \langle a^4 b\rangle, \langle ab\rangle, \langle a^3 b\rangle \}$

$\therefore$ all 5 Sylow 2-subgroups are conjugate to each other.

Under conjugation with elements of $P = \langle b\rangle$ we find the P-orbits:

$orb(\langle b\rangle) = \{\langle b\rangle\}$ $\quad \therefore |orb(\langle b\rangle)| = 1 = 2^0$

$orb(\langle a^2 b\rangle) = \{\langle a^2 b\rangle, \langle a^3 b\rangle\}$ $\quad |orb(\langle a^2 b\rangle)| = 2 = 2^1$

$orb(\langle a^4 b\rangle) = \{\langle a^4 b\rangle, \langle ab\rangle\}$ $\quad |orb(\langle a^4 b\rangle)| = 2 = 2^1$

N.B. $|P_c| = 1 \bmod p$ indeed $|P_c| = 5$.

D_5 also has a Sylow 5-subgroup with $n_5 = 1$ or 6; n_5 divides 2 $\therefore n_5 = 1$

hence $\langle a\rangle \cong \mathbb{Z}_5 \subset D_5$ is a normal subgroup.

Appendix

A Equivalence relations

Definition A.1. A binary operation on a set X is said to be an **equivalence relation**, if and only if it is reflexive, symmetric and transitive. That is for all $a, b, c \in X$:

- Reflexivity: $a \sim a$;
- Symmetry: $a \sim b$ if and only if $b \sim a$;
- Transitivity: if $a \sim b$ and $b \sim c$ then $a \sim c$.

A.1 Equivalence classes

Theorem A.1. If $\sim$ is an equivalence relation on a set X and $x, y \in X$ then, these statements are equivalent:

- $x \sim y$;
- $[x] = [y]$;
- $[x] \cap [y] = \emptyset$

B Functions

B.1 Well-defined maps

Definition B.1. A map is said to be **well-defined** if and only if the map is **not** a **many-to-one** map.

> **Note B.1.** In a well-define map an element from the domain **cannot** be mapped to two or more elements in the range.

B.2 Injectivity

Definition B.2. A function $f : X \to Y$ is **injective** (or **one-to-one**) if every element $f(x) \in B$ is mapped to by at most one element in the domain A. An injective function is called an **injection**.

With symbols, a function $f : A \to B$ is called **injective** if, for all $x_1, x_2 \in X, f(x_1) = f(x_2)$ implies that $x_1 = x_2$.

> **Note B.2.** To show that a function is injective, first suppose that $f(x_1) = f(x_2)$ then show by direct implication that $x_1 = x_2$.

Example B.1. Show that the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 5x - 3$ is injective.
Solution: Suppose that $f(x_1) = f(x_2)$; then we have

$$\begin{aligned} & f(x_1) = f(x_2) \\ \Rightarrow\ & 5x_1 - 3 = 5x_2 - 3 \\ \Rightarrow\ & x_1 = x_2. \end{aligned}$$

Thus, f is injective.

Theorem B.1. A function f is injective if and only if every horizontal line intersects the graph of f no more than once.

B.3 Surjectivity

Definition B.3. A function $f : X \to Y$ is **surjective** (or **onto**) if every element in B is mapped to by at least one element of A. A surjective function is called a **surjection**.

In symbols, a function $f : X \to Y$ is called **surjective** if for all $y \in Y$ there exists $x \in X$ such that $f(x) = y$.

Example B.2. Show that the map $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$ is surjective.
Solution: Suppose $y \in \mathbb{R}$. We require that $f(x) = y$, i.e. $x^3 = y$ thus, we can take $x = \sqrt[3]{y}$. We rewrite the proof. Suppose that $y \in \mathbb{R}$. Then let $x = \sqrt[3]{y}$ we have

$$\begin{aligned} f(x) &= f(\sqrt[3]{y}) \\ &= (\sqrt[3]{y})^3 \\ &= y. \end{aligned}$$

Thus, f is surjective.

B.4 Bijections

Definition B.4. A function $f : A \to B$ is **bijective** if it is both surjective and injective. A bijective function is called a **bijection**.