5CCM232A
Groups and Symmetries Lecture Notes

Authors: G. Papadopoulos, B. Doyon, P. P. Cook and many others over the years[1].

(Notes typed by B. Doyon and P. P. Cook)

Department of Mathematics, King's College London.

15th April 2024

[1] For comments on the lecture notes and for weeding out typos, thanks are due to to Frederick Eidsnes Thogersen, Senan Sekhon, Jordan Hofman, Pol Van Hoften, Alexander Stokes, Paul Weinreb, Dean Yates, Ana Dias Frias, Eylul Zorba, Loukas Grimanellis, Zhibo Liu, Seyed Ali Sadreddin Yasavol, Hao Wen, Junlin Mo, Zhiping She, and Jingchun Xu.

0. Contents

1. Basics

Definition 1.1. *A group is a set G and a mapping from the Cartesian product $G \times G$ into G (a* law of composition *or* multiplication law*), which we will denote by juxtaposition*

$$G \times G \to G \quad : \quad (g_1, g_2) \mapsto g_1 g_2, \tag{1.1}$$

with the following properties:

(i) Associativity: $g_1(g_2 g_3) = (g_1 g_2) g_3$ for all $g_1, g_2, g_3 \in G$

(ii) Identity: there exists $e \in G$, called an identity, such that $ge = eg = g$ for all $g \in G$

(iii) 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.

Comment(s). *(On the definition of a group.)*

1. *The Cartesian product is the combination of two sets U and V such that its elements are combined in pairs to form elements of $U \times V$. The most common example is the Cartesian coordinates used to denote elements of the Cartesian plane $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ where for $x, y \in \mathbb{R}$ then $(x, y) \in \mathbb{R} \times \mathbb{R}$ is a single element in the Cartesian product of $\mathbb{R}$ with $\mathbb{R}$.*

2. *The order of multiplication is normally important, typically (but not always) $g_1 g_2 \neq g_2 g_1$.*

3. *It is commonplace to use a special notation (often a dot $\cdot$ or a circle $\circ$) to indicate group multiplication, e.g. sometimes you might see $g_1 \circ g_2$ or $g_1 \cdot g_2$ for a group product. Throughout this course we will use juxtaposition of group elements to denote group multiplication i.e. $g_1 \circ g_2 = g_1 \cdot g_2 = g_1 g_2$.*

4. *The identity e is unique (prove this).*

5. *Given any $g \in G$ its inverse g^{-1} is unique (prove this).*

6. $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$ *for all* $g_1, g_2 \in G$ *(prove this).*

7. $(g^{-1})^{-1} = g$ *for all* $g \in G$ *(prove this).*

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

Definition 1.3. *If* $g_1g_2 = g_2g_1$ *for all* $g_1, g_2 \in G$*, 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*

(i) $h_1h_2 \in H$ *for all* $h_1, h_2 \in H$ *and*

(ii) $h^{-1} \in H$ *for all* $h \in H$.

Example 1.1. *Some examples of groups are*

- $\mathbb{R}$ *under addition;*
- $\mathbb{Z}$ *under addition (subgroup of* $\mathbb{R}$*);*
- $\mathbb{Z}_p$*: the integers under addition modulo* $p \in \mathbb{N}$*;*
- $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ *under multiplication;*
- $\mathbb{R}^+ := \{x : x > 0\}$ *under multiplication (subgroup of* $\mathbb{R}^*$*);*
- $\{2^n : n \in \mathbb{Z}\}$ *under multiplication;*
- *the matrices* $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R},\ ad - bc \neq 0 \right\}$ *under matrix multiplication;*
- *the affine maps* $\{\{\mathbb{R} \to \mathbb{R} : x \mapsto f(x) = ax + b\} : a \in \mathbb{R}^*,\ b \in \mathbb{R}\}$ *under map composition.*

2. The Cyclic Groups

2.1 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 ($n \in \mathbb{Z}$) is defined as follows: it is the n-times product of g with itself, $gg \dots g$ (n times), for $n > 0$; it is the $|n|$-time product of g^{-1} with itself for $n < 0$; and it is e if $n = 0$. Consequently

$$g^{m+n} = g^m g^n, \quad (g^m)^n = g^{mn} \quad \forall \quad m, n \in \mathbb{Z}. \tag{2.1}$$

Let G be a group. The set generated by $g \in G$, denoted $\langle g \rangle$, is the set of all powers of g:

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}. \tag{2.2}$$

Observe that $\langle g \rangle$ is a subgroup of G. Indeed by (2.1), the inverse of g^n is g^{-n} for all $n \in \mathbb{Z}$ and the set is closed under the composition law of G (the last two statements thanks to (2.1)). Observe that the subgroup $\langle g \rangle$ is abelian: $g^m g^n = g^{m+n} = g^{n+m} = g^n g^m$ for all $m, n \in \mathbb{Z}$. The subgroup $\langle g \rangle$ is the intersection of all subgroups of G that contain the element g.

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

We note that a cyclic group is abelian.

Example 2.1.

- *$\mathbb{Z}$ under addition is a cyclic group. It has two generating elements: 1 and -1, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.*
- *The group $\{2^n : n \in \mathbb{Z}\}$ under multiplications is a cyclic group, with generating elements 2 and $1/2$.*
- *The group $\mathbb{Z}_p$ is a cyclic group. For instance: $\mathbb{Z}_2 = \{0, 1\} = \langle 1 \rangle$. $\mathbb{Z}_3 = \{0, 1, 2\} = \langle 1 \rangle = \langle 2 \rangle$. $\mathbb{Z}_4 = \{0, 1, 2, 3\} = \langle 1 \rangle = \langle 3 \rangle$, but $\mathbb{Z}_4 \neq \langle 2 \rangle$. In general, if p is prime, then $\mathbb{Z}_p = \langle n \rangle$ for all $n \in \{1, 2, \dots, p-1\}$ (show this!).*

- *Given a positive integer n, the group $\{e^{2\pi ik/n} : k = 0, 1, \dots, n-1\}$ under multiplications is cyclic, and equal to $\langle e^{2\pi i/n}\rangle$.*

Let us consider for a while groups of finite order only, that is, $|G| < \infty$. The next theorem tells us more precisely about the structure of cyclic groups.

Theorem 2.1. *Let G be a cyclic group generated by g_0. Then*

(a) g_0^n, $n = 0, 1, 2, \dots, |G| - 1$ are all distinct elements, and

(b) $g^{|G|} = e$ for all $g \in G$.

Proof. We prove (a) by contradiction. Suppose there exists n_1, n_2 with $0 \le n_2 < n_1 \le |G| - 1$ and $g_0^{n_1} = g_0^{n_2}$. Then $g_0^{n_1 - n_2} = e$. Denote $q = n_1 - n_2$, note that $0 < q < |G|$. Now we may write any integer n as $n = kq + r$ for $k \in \mathbb{Z}$ and (remainder) $r = 0, \dots, q-1$. Hence $g_0^n = g_0^{kq+r} = (g_0^q)^k g_0^r = e^k g_0^r = g_0^r$. Therefore in $\langle g_0\rangle$ there are q elements (the number of possible values of r), i.e. $q = |G|$ which contradicts the statement $q < |G|$ deduced from our assumptions. Hence there is no pair of integers $0 \le n_2 < n_1 \le |G| - 1$ such that $g_0^{n_1} = g_0^{n_2}$ and all elements of $\langle g_0\rangle$ are distinct.

To prove (b), as all $|G|$ elements are distinct (by part (a)) then $g_0^{|G|} = g_0^m$ for some $m \in \{0, 1, 2, \dots, |G| - 1\}$. Hence $g_0^{|G|-m} = e$, but now if $m > 0$, this contradicts (a), hence $m = 0$ and $g_0^{|G|} = e$. Finally, as for every $g \in G$ there exists n such that $g = g_0^n$, we have $g^{|G|} = (g_0^n)^{|G|} = g_0^{n|G|} = (g_0^{|G|})^n = e^n = e$. □

Theorem 2.2. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $H \subset G = \langle a\rangle = \{e, a, a^2, \dots, a^{|G|-1}\}$ be a subgroup. Let q be the smallest non-zero, positive integer such that $a^q \in H$. Let $c \in H$. By cyclicity of G, there is a $n \in \mathbb{Z}$ such that $c = a^n$. We have $n = kq + r$ for unique $k \in \mathbb{Z}$ and $r \in \{0, \dots, q-1\}$, hence $c = (a^q)^k a^r$. Since H is a subgroup, $a^{-kq} \in H$ and $a^{-kq}c \in H$, which implies that $a^r \in H$. Hence $r = 0$ or $r \ge q$ since q is the minimal integer such that $a^q \in H$, which implies $r = 0$ by definition of r. Hence, $c = a^{kq} = (a^q)^k$. This is true for every $c \in H$, so $H = \langle a^q\rangle$, and H is cyclic. □

2.2 Symbols and Relations

The notion of generating elements can be generalised to more than one element. Let $a, b \in G$. The set $\langle a, b\rangle$ is the set of all powers of a and b and all products thereof with any number of factors. It is a subgroup of G and it is the intersection of all subgroups that contain both a and b. If $G = \langle a, b\rangle$, then we say that a, b generate the group G and the set $\langle a, b\rangle$ is frequently called the ‘span’ of a and b. One can generalise this to more elements.

We may understand the general principle using symbols and relations. Consider an alphabet of two letters: $\{e, a\}$. Let us consider all words that we can form from these: e, a, ea, aa, a^3e, aea, etc. This is a set with a multiplication law: the *concatenation* of words, e.g. a multiplied with ea gives aea. The multiplication law is automatically associative (easy to check). But this does not yet form a group.

Let us now impose some relations. The "trivial" ones, that we will always impose implicitly when looking at symbols and relations, are those having to do with the identity element: $e^2 = e$ and $ea = ae = a$. That reduces the words we can form: $ea = a$, $aea = a^2$, etc. It also guarantees that we now have a set not only with an associative multiplication law, but also with an identity element, the word e. But this does not yet form a group.

The words we have now are e, a, a^2, a^3, a^4, etc. Let us impose one more relation: $a^n = e$ for some fixed positive integer n (e.g. for $n = 4$). This unique additional relation reduces further the number of words we can make, and now we have a group. Take $n = 4$ for instance. We now have e, a, a^2, a^3 and nothing else (any other word reduces to one of these four). This now forms a group: we can check that every element has an inverse $a^{-1} = a^3$, $(a^2)^{-1} = a^2$, and $(a^3)^{-1} = a$. It is a cyclic group, generated by a, so it is the group $\langle a\rangle$ (with the additional relation $a^4 = e$ implied).

We could instead think of having two non-trivial symbols (three symbols with the identity e): a, b. Let us impose, besides the trivial relations involving e, two additional relations: $ab = ba = e$. Again, this is sufficient to make this into a group. We have $a^{-1} = b$, and the group formed is again cyclic; it can be generated either by a or by b (it is the group $\langle a\rangle = \langle b\rangle$).

It is always possible to describe groups by giving an alphabet and a set of relations. Non-cyclic groups will be generated by more than one symbol; the tutorial problem gives an example.

3. Maps and Permutation Groups

Let us recall some fundamental ideas. Consider two sets X, Y and a map $f : X \to Y$. As usual we write $y = f(x)$ for the value in Y that is mapped from $x \in X$.

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

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

Definition 3.3. *The map f is onto (or surjective) 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 one-to-one (or injective) if for all $y \in f(X)$ there exists a unique $x \in X$ such that $y = f(x)$. That is, if the following proposition holds: $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ (denoted $f : X \rightarrowtail Y$).*

Definition 3.5. *A map f that is one-to-one and onto is called bijective.*

If $f : X \to Y$ is bijective, then there is a unique correspondence between X and Y: for every $y \in Y$ there is a unique $x \in X$ such that $y = f(x)$, and for every $x \in X$ there is a unique $y \in Y$ such that $y = f(x)$. We can define an inverse map $f^{-1} : Y \to X$ via this unique correspondence such that

$$f(f^{-1}(y)) = y, \quad f^{-1}(f(x)) = x \quad \forall \quad y \in Y,\ x \in X. \tag{3.1}$$

The inverse map is itself bijective (proofs omitted).

Given two maps f, g from X to X, we can form a third by composition: $h = f \circ g$ given by $h(x) = f(g(x))$. Consider the set $Map(X, X)$ all such maps. Then: 1) if f and g are such maps, then $f \circ g$ also is; 2) given $f, g, h \in Map(X, X)$, we have that $(f \circ g) \circ h = f \circ (g \circ h)$; 3) $Map(X, X)$ contains the identity which we will denote id; this is the map $\mathrm{id} : X \to X,\ x \mapsto \mathrm{id}(x) = x$. It has the properties that $f \circ \mathrm{id} = \mathrm{id} \circ f = f$ for all $f \in Map(X, X)$. In order to have a group, we thus need only one more property: the existence of inverses.

Theorem 3.1. *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, $Perm(X)$.*

Proof. We only need to check that inverses exist as we have already argued that the other properties of a group are satisfied for $Map(X, X)$. For every bijective map f, f^{-1} exists and is bijective. Hence f^{-1} is an element of the group. It has the property that $f^{-1} \circ f = f \circ f^{-1} = \text{id}$ thanks to equation (3.1). □

Comment(s). *Note that in defining a permutation group on a set X, we have not needed to consider* all *maps in $Map(X, X)$ but just a subset that satisfy closure, which we have called the span of a set of bijective maps in the theorem above.*

Let X be a finite (or even countable) set. We may label its elements by positive integers $1, 2, \ldots$. Using this labelling, an element of $Perm(X)$ can be seen as a map from the positive integers to the positive integers, $k \mapsto i_k$ for $k = 1, 2, \ldots$, with the conditions that all integers i_k are distinct and that for every label k, there exists a k' such that $i_{k'} = k$ (so that the map is bijective). If the set is finite, say $k \in \{1, 2, \ldots, n\}$, then the requirements are that all integers i_k be distinct, and that $i_k \in \{1, 2, \ldots, n\}$ for all k.

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

Comment(s). *On the symmetric group and permutations.*

1. *We can denote elements of S_n by $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ which denotes the map $1 \mapsto i_1$, $2 \mapsto i_2$, $\ldots n \mapsto i_n$.*

2. $|S_n| = n!$

3. *E.g. S_3 is symmetric group of all permutations of three elements. It has $3! = 6$ elements and consists of the permutations:*

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

4. *One could define S_3 in terms of symbols and relations as:*

$$S_3 = \{\langle a, b\rangle | a^3 = e, b^2 = e, ab = ba^2\}.$$

(Check that $ab = ba^2$ for S_3 as defined in point 3 above.) Note that as $ab \neq ba$ so S_3 is a non-abelian group.

5. *Permutations can be presented in cycle notation where* $(i_1 i_2 i_3 \ldots i_n)$ *denotes the permutation that maps* $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots i_{n-1} \mapsto i_n$ *and* $i_n \mapsto i_1$*. Hence* (123) *and* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *denote the same permutation.* $(i_1 i_2 i_3 \ldots i_n)$ *is called an n-cycle and* (123) *is a 3-cycle.*

6. *In general a single permutation may be written as multiple cycles on separate sets of elements. For example* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ *written in cycle notation consists of a 3-cycle and a 2 cycle denoted, for example, by* $(123)(45)$*.*

7. *To convert a permutation written in the form* $\begin{pmatrix} 1 & 2 & 3 & \ldots n \\ i_1 & i_2 & i_3 & \ldots i_n \end{pmatrix}$ *to cycle notation, one can start with the label* 1 *and follow its mapping under repeated action of the permutation: the cycle containing* 1 *is the list of elements that* 1 *is mapped to under the repeated action of the permutation. This procedure for constructing the cycles is repeated until every element in the set is contained in some cycle. For example consider* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$*, as* $1 \mapsto 5 \mapsto 1$, $2 \mapsto 3 \mapsto 2$ *and* $4 \mapsto 4$*, the permutation is* $(15)(23)(4)$*. In practise 1-cycles are usually neglected when using cycle notation so* $(15)(23)$ *denotes the permutation in this example.*

8. *A 2-cycle such as* (12) *is called a transposition and every permutation can be re-written as a product of transpositions e.g.* $(123) = (12)(23)$ *(check this!).*

9. *Despite the convention of omitting one-cycles, sometimes it is mathematically interest to take them into account. For example we need the one cycles in order to denote the identity element in* S_3*:*

$$S_3 = \{(1)(2)(3), (123), (132), (12)(3), (1)(23), (13)(2)\}.$$

Note that there is a relation between the permutations in S_3 *and the integer partitions of three:* S_3 *contains one* $1+1+1$*-cycle, two* 3*-cycles and three* $1+2$*-cycles (compare this with the integer partitions of three:* $3 = 1+1+1 = 1+2 = 3$*). In general a permutation in* S_n *can be written as a product of* n_j *j-cycles where* $n = \sum_j j n_j$*, e.g. for* $(12)(3)$ *we have* $n_1 = 1$ *and* $n_2 = 1$ *so that* $\sum_j j n_j = 1 + 2 = 3$*, so* $(12)(3)$ *is a permutation in* S_3*. In fact the number of partitions of* n *with the same cycle structure is* $N = \frac{n!}{\Pi_j j^{n_j} n_j!}$*, for example in* S_3 *we constructed three* $1+2$*-cycles - each one has* $n_1 = 1$ *and* $n_2 = 1$ *so* $N = \frac{3!}{1^1(1!)2^1(1!)} = \frac{6}{2} = 3$*.*

10. *An even permutation is defined as one which can only be written as the product of an even number of transpositions, while an odd permutation is one that can only be written using an odd number of transpositions. For example* $(1)(2)(3)$ *involves zero transpositions, so is an even permutation;* $(123) = (12)(23)$ *is an even permutation; and* $(1)(23) = (23)$ *is an odd permutation. In all* S_3 *contains three even permutations and three odd permutations.*

11. *The alternating group* A_n *is a subgroup of* S_n *consisting of all the even permutations in* S_n*. This is always half of the permutations in* S_n*, hence* $|A_n| = \frac{n!}{2}$*. For example* $A_3 = \{(1)(2)(3), (123), (132)\} = \{e, a, a^2\} \cong \mathbb{Z}_3$*.*

4. Homomorphisms and isomorphisms

Definition 4.1. *Let G_1 and G_2 be groups. A map $\phi : G_1 \to G_2$ is a homomorphism if $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in G_1$.*

Comment(s). *(On the definition of a homomorphism.)*

1. *In other words ϕ preserves the structure of a group as gh is mapped to $\phi(g)\phi(h)$.*

2. *Note that a homomorphism distributes over a product of group elements, but it is a map from one group G_1 to another G_2 so that the group multiplication law is different on each of the definition of the homorphism (on the left gh are multiplied using the group law of G_1 while on the right $\phi(g)\phi(h)$ are multiplied using the multiplication law of G_2).*

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

Equivalently, a map $\phi : G_1 \to G_2$ is an isomorphism if it is bijective and if it satisfies $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in G_1$.

As a trivial example, the identity map $\mathrm{id} : G \to G$ is always an isomorphism of a group onto itself.

Theorem 4.1. *Let ϕ be a homomorphism from G_1 to G_2 and e_1, e_2 be the identity elements in G_1 and G_2 respectively, then,*

(i) $\phi(e_1) = e_2$ *and*

(ii) $\phi(g^{-1}) = \phi(g)^{-1}\ \forall\ g \in G_1$.

Proof. (i) Since $e_1e_1 = e_1$ then $\phi(e_1) = \phi(e_1e_1) = \phi(e_1)\phi(e_1)$. Multiplying by the inverse element $\phi(e_1)^{-1}$ in G_2 and we have $\phi(e_1)\phi(e_1)^{-1} = \phi(e_1)\phi(e_1)\phi(e_1)^{-1}$, hence $e_2 = \phi(e_1)$. (ii) Now consider $e_1 = gg^{-1}$ for $g \in G_1$. Then using the previous result, we find $e_2 = \phi(e_1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$, and pre-multiplying by the inverse element $\phi(g)^{-1}$ in G_2 we have $\phi(g)^{-1} = \phi(g)^{-1}\phi(g)\phi(g^{-1}) = \phi(g^{-1})$. □

Example 4.1. *A homomorphism from S_2 to S_3:*

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Note this is not an isomorphism. Could one construct an isomorphism from S_2 to S_3?

Definition 4.3. *Two groups G_1 and G_2 are isomorphic if there exists an isomorphism $\phi : G_1 \to G_2$.*

Theorem 4.2. *The "isomorphic" relation is an equivalence relation, which we will denote by $\cong$.*

Proof. We need to check that the relation is reflexive, symmetric and transitive.

Reflexive: a group is isomorphic to itself because the identity map id is an isomorphism.

- Reflexive: $G \cong G$ as the identity map is an isomorphism mapping G to itself.

- Symmetric: we must show that if $\phi : G_1 \twoheadrightarrow G_2$ is an isomorphism, than so is $\phi^{-1} : G_2 \twoheadrightarrow G_1$. We know that ϕ^{-1} is a bijective map from G_2 onto G_1, so we must check that it is a homomorphism. Let $g = \phi(h), g' = \phi(h') \in G_2$ with $h, h' \in G_1$ (h and h' always exist because ϕ is a bijection). Then $\phi^{-1}(gg') = \phi^{-1}(\phi(h)\phi(h')) = \phi^{-1}(\phi(hh')) = hh'$ where in the penultimate step we have used that ϕ preserves the multiplication law. This equals $hh' = \phi^{-1}(g)\phi^{-1}(g')$ by the definition of ϕ^{-1}. Hence $\phi^{-1}(gg') = \phi^{-1}(g)\phi^{-1}(g')$ so ϕ^{-1} is a homomorphism.

- Transitive: let ϕ' and ϕ be isomorphisms. We need to show that $\phi' \circ \phi$ is an isomorphism. Certainly $\phi' \circ \phi$ is bijective, so we need to shown that it is a homomorphism. We have $\phi' \circ \phi(gg') = \phi'(\phi(gg')) = \phi'(\phi(g)\phi(g')) = \phi'(\phi(g))\phi'(\phi(g')) = \phi' \circ \phi(g)\, \phi' \circ \phi(g')$ so $\phi' \circ \phi$ preserves the multiplication law.

□

If two groups are isomorphic, then they are structurally the same group. For instance, if $G_1 \cong G_2$, then: $|G_1| = |G_2|$; G_1 abelian $\Leftrightarrow$ G_2 abelian; etc. Further, isomorphisms preserve the order of elements:

Definition 4.4. *The order of an element a in a group G is the smallest positive integer k such that $a^k = e$.*

Clearly by Theorem 2.1, $|\langle a \rangle|$ is equal to the order of a. Let $\phi : G_1 \to G_2$ be an isomorphism onto G_2, and let $g_1 \in G_1$. Now $\phi(\langle g_1 \rangle) = \langle \phi(g_1) \rangle$ as $\phi(g_1^{n+1}) = \phi(g_1^n g_1) = \phi(g_1^n)\phi(g_1)$ (as ϕ is a homomorphism) for all $n \geq 0$, and then by induction $\phi(g_1^n) = \phi(g_1)^n$.

Theorem 4.3. *Two cyclic groups of the same order are isomorphic.*

Proof. Let $G_1 = \langle g_1 \rangle$ and $G_2 = \langle g_2 \rangle$, and $N = |G_1| = |G_2|$ where N is finite. By Theorem 2.1, we have $G_1 = \{g_1^0, g_1^1, \ldots, g_1^{N-1}\}$ and $G_2 = \{g_2^0, g_2^1, \ldots, g_2^{N-1}\}$ as sets. Let us define the map $\phi : G_1 \to G_2$ by $\phi(g_1^n) \mapsto g_2^n$ for all $n \in \mathbb{Z}$. We will show that this is an isomorphism. It is bijective by construction. To show it is a homomorphism, consider $\phi(g_1^m g_1^n) = \phi(g_1^{m+n}) = g_2^{m+n} = g_2^m g_2^n = \phi(g_1^m)\phi(g_1^n)$.

Here we did the case of cyclic groups of finite orders; the case of infinite (countable) cyclic groups can be done similarly. □

Given the above theorem, when discussing cyclic groups, it is sufficient to discuss $\mathbb{Z}_n$ (for $n = 2, 3, 4, \ldots$) and $\mathbb{Z}$, as any cyclic group will be isomorphic to one of these.

Example 4.2. *Let $G_1 = \{1, -1\}$ under multiplication of integers, and*

$$G_2 = S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

Consider the function

$$\phi(1) = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \text{and} \qquad \phi(-1) = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

The map is clearly bijective. Also,

$$\phi((-1)\cdot(-1)) = \phi(1) = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \phi(-1)\phi(-1),$$

and $\phi(1) = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ hence ϕ maps identity to identity. This is sufficient to conclude that ϕ is an isomorphism.

Example 4.3. *Let $G_1 = \mathbb{Z}_n$ and $G_2 = \{e^{2\pi ik/n} : k = 0, 1, \ldots, n-1\}$. Consider the map $\phi : G_1 \to G_2$ given by $\phi(k) = e^{2\pi ik/n}$, $k = 0, 1, 2, \ldots, n-1$. It is well-defined: since we restrict to k between 0 and $n-1$, they are all different integers when taken mod n. It is surjective: just by definition, we get all $e^{2\pi ik/n} : k = 0, 1, \ldots, n-1$. It is injective: if $\phi(k) = \phi(k')$ then $e^{2pii(k-k')/n} = 1$ hence $k - k' = 0 \mod n$ so that $k = k' \mod n$. Further, we have $\phi(k + k' \mod n) = e^{2\pi i(k+k' \mod n)/n} = e^{2\pi i(k+k')/n} = e^{2\pi ik/n}e^{2\pi ik'/n} = \phi(k)\phi(k')$.*

5. Cosets and Lagrange's Theorem

Let H be a subgroup of G. Now define a relation $\sim$ in G as follows: a is equivalent to b, i.e. $a \sim b$, iff $ab^{-1} \in H$. This is an equivalence relation.

Proof. We need to check reflexivity, symmetry, transitivity.

- Reflexive: $a \sim a$. Indeed, $aa^{-1} = e \in H$ as the identity is in any subgroup.
- Symmetric: $a \sim b \Rightarrow b \sim a$. Indeed, $ab^{-1} \in H$ implies that $(ab^{-1})^{-1} \in H$ as every element of a subgroup has an inverse in the subgroup, whence $ba^{-1} \in H$.
- Transitive: $a \sim b,\ b \sim c \ \Rightarrow\ a \sim c$. Indeed if $ab^{-1} \in H$ and $bc^{-1} \in H$ then their product is in H as a subgroup is closed, so $ab^{-1}bc^{-1} \in H$ implying $ac^{-1} \in H$.

□

The equivalence class of a is denoted $[a] := \{b \in G : a \sim b\}$. Clearly, if $a \sim b$ then $[a] = [b]$: if $c \sim a$ then $c \sim b$ by transitivity ($[a] \subset [b]$) and if $c \sim b$ then $c \sim a$ by transitivity ($[b] \subset [a]$). Let us denote by Ha the set $\{ha : h \in H\}$, then, as will be shown, $[a] = Ha$.

Proof. If $b \sim a$ then $ba^{-1} \in H$ hence there exists $h = ba^{-1} \in H$ such that $b = ha$; this implies $[a] \subset Ha$. While if $c = ha \in Ha$ for some $h \in H$, then $ca^{-1} = h \in H$ then $c \sim a$ for all $c \in Ha$ and therefore $Ha \subset [a]$. Together $[a] \subset Ha$ and $Ha \subset [a]$ imply $[a] = Ha$. □

Definition 5.1. *The set of equivalent classes $\{Ha : a \in G\}$ 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.*

Note that the element of G is to the right of the element of H, hence the name "right coset".

We could have made a similar construction but using a different equivalence relation in G defined by $a \sim b$ iff $a^{-1}b \in H$. Under this equivalence relation, $[a] = aH$. The equivalence classes are the left cosets:

Definition 5.2. *The set of equivalent classes $\{aH : a \in G\}$ is the set of left cosets of G with respect to H.*

Hence we have two types of cosets (right and left), with two types of equivalence relations. For now we will derive results for right cosets, but similar results hold for left cosets. Later on we will concentrate on left cosets.

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

In fact this is true for two equivalence classes of any given equivalence relation.

Proof. Let $a, b \in G$. If $[a]$ and $[b]$ have no element 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 $[a] = [b]$ by the statement shown above. □

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

Proof. Fix $a \in G$, and consider its right coset Ha. We will show that this has the same number of elements as H itself. Since this holds independently of a, this will show the theorem. Consider the map $M : H \to Ha$, $h \mapsto ha$. We just need to show that it is a bijection. Given any $b \in Ha$, we have $b = ha$ for some $h \in H$, hence $b = M(h)$, so M is onto Ha. Further, if $M(h) = M(h')$ then $ha = h'a$ hence $haa^{-1} = h'aa^{-1} \Rightarrow h = h'$ so M is injective. □

Definition 5.3. *The number of cosets of G wrt H is called the index of H in G, which we will denote $i(H, G)$.*

Theorem 5.3. *(Lagrange's Theorem) Let H be a subgroup of G. The order of H divides the order of G i.e. $|G| = |H|\, i(H, G)$.*

Proof. We have to show that the right cosets of G w.r.t. H form an equipartition of G into $i(H, G)$ disjoint subsets all with exactly $|H|$ elements. This follows from three facts: the union of all right cosets, $\cup_{a\in G} Ha$, is G itself; two right cosets Ha and Ha' are either disjoint or identical; and each right coset has the same number of element $|H|$. The last two statements are Theorems 5.1 and 5.2. So we just need to prove the first. Note that $a \in Ha$; indeed, $e \in H$, hence $a = ea \in Ha$. This implies that $\cup_{a\in G} Ha = G$. □

Definition 5.4. *A proper subgroup of a group G is a subgroup $H \subset G$ that is different from the trivial group $\{e\}$ and from G itself.*

Corollary 5.0.1. *If $|G|$ is prime, then the group G has no proper subgroup.*

Proof. If H is a proper subgroup of G, then $|H|$ divides $|G|$ and $|H|$ is a number not equal to 1 or $|G|$. Contradiction. □

Corollary 5.0.2. *Let $a \in G$ and let k be the order of a. Then k divides $|G|$.*

Proof. Let us look at the cyclic subgroup $\langle a \rangle$ of G generated by a. By Theorem 2.1 this has order k. Hence k divides $|G|$. □

Corollary 5.0.3. *If $|G|$ is prime then G is a cyclic group.*

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

From the latter corollary, observe that any group of prime order is unique up to isomorphisms.

Example 5.1. *Take the group $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$ with the relations written previously, $a^3 = e, \quad b^2 = e, \quad ab = ba^2, \quad a^2b = ba$. Take the subgroup $H = \{e, a, a^2\}$. Let us calculate all the right cosets associated to this subgroup. We have*

$$He = H, \quad Ha = \{a, a^2, a^3 = e\} = H, \quad Ha^2 = \{a^2, a^3 = e, a^4 = a\} = H$$

and

$$Hb = \{b, ab, a^2b\}, \quad Hab = \{ab, a^2b, a^3b = b\} = Hb, \quad Ha^2b = \{a^2b, a^3b = b, a^4b = ab\} = Hb.$$

Hence we find that any two cosets Hg_1 and Hg_2 for $g_1, g_2 \in G$ are either disjoint or identical. We find that there are exactly 2 different cosets occurring, which are the sets H and Hb. This is in agreement with Lagrange's theorem, because $|G| = 6$, $|H| = 3$ so that the number of different cosets should be $i(H, G) = |G|/|H| = 2$, which it is.

Example 5.2. *Consider again $G = S_3 = \{e, a, a^2, b, ab, a^2b\}$ with the relations as before. Consider the subgroup $H = \{e, b\} = \langle b \rangle$. We have $Ha = \{a, a^2b\}$, $Ha^2 = \{a^2, ab\}$. We have 3 cosets, each containing 2 elements, giving a total of 6 elements.*

6. Groups of Low Order and Klein's Four-Group

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

- $|G| = 1$: there is only one possibility because the identity must always be there, so $G = \{e\}$.

- $|G| = 2$: $G = \{e, a\}$ with $a \neq e$. Since 2 is prime, by corollary (iii) of Theorem 5.3 G must be cyclic, and by Theorem 4.3, it must be isomorphic to $\mathbb{Z}_2$, hence we must have $a^2 = e$. Let us deduce that from first principles. The inverse of a must exist. It cannot be e because $ae = a \neq e$, so we must have $a^{-1} = a$. Hence $e = aa^{-1} = a^2$.

- $|G| = 3$: Again, since 3 is prime, G must be cyclic (hence isomorphic to $\mathbb{Z}_3$, so we can always write $G = \{e, a, a^2\}$ with $a^3 = e$. It could likewise be deduced from first principles.

- $|G| = 4$: $G = \{e, a, b, c\}$ (all distinct). We know that $\langle a \rangle$, for instance, is a subgroup, so its order divides 4. Hence there are 2 or 4 elements in $\langle a \rangle$. By Theorem 2.1, this means that $a^2 = e$ or $a^4 = e$. In the latter case, $\langle a \rangle = G$, so G is cyclic (hence isomorphic to $\mathbb{Z}_4$). Let us assume that G is not cyclic, in order to see what other group we can have. So $a^2 = e$. We can then do the same for b and c, and always assuming that G is not cyclic, we have $a^2 = b^2 = c^2 = e$. Then consider ab, and check, for the various possibilities, if associativity holds.

  1. $ab = a$: $(a^2)b = b$ and $a(ab) = a^2 = e$, no.
  2. $ab = b$: similarly, no.
  3. $ab = e$: $a(ab) = a$ and $(a^2)b = b$, no.

  Hence if the group exists, we must have $ab = c$. Similarly, we must have $ba = c$, $bc = cb = a$ and $ca = ac = b$. To show existence of the group, must check associativity in all possible triple products abc, a^2b, etc. (left as exercise; it's a consequence of the matrix representation below).

The above arguments show:

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

N.B. This is a Cayley table: the entry in row g_r and column g_c is $g_r g_c$, it shows the results of all multiplications in the group featuring two elements.

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

Comment(s). *(On the Klein four-group.)*

1. *Both the cyclic group and the group V_4 are abelian. Hence there are no non-abelian groups of order less then or equal to 4. By Corollary (iii) of Theorem 5.3, any group of order 5 is also cyclic hence abelian, so there are no non-abelian groups of order less then or equal to 5.*

2. *The group V_4 is the smallest non-cyclic group.*

3. *V_4 is such that all elements different form e have order 2.*

4. *V_4 has 5 subgroups: the trivial one and V_4 itself, as well as the 3 proper subgroups $\langle a\rangle$, $\langle b\rangle$ and $\langle c\rangle$.*

5. *V_4 can be seen as a subgroup of S_4:*

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

6. *V_4 can also be described using symbols and relation. It is generated by the symbols a, b, with the relations $a^2 = b^2 = e$ and $ab = ba$. We have $V_4 = \langle a, b\rangle = \{e, a, b, ab\}$.*

Example 6.1. *A matrix representation of V_4: Consider the 2×2 matrices*

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

and the product rules on these matrices given by the usual matrix multiplication. These form the group V_4.

Example 6.2. *Cosets on V_4: Take $V_4 = \{e, a, b, ab\}$ with the relations shown above. A (cyclic) subgroup is of course $H = \{e, a\} = \langle a \rangle$. One coset is $H = Ha$, the other is $Hb = \{b, ab\}$. They have no element in common, and have the same number of elements. Lagrange's theorem holds.*

7. Direct products

Definition 7.1. *Let G_1 and G_2 be two groups. Then $G = G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1,\ g_2 \in G_2\}$ is a group, with the multiplication law $(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$. $G_1 \times G_2$ is called the direct product of G_1 and G_2*

Exercise 7.1. *Confirm that the axioms of a group are satisfied by the direct product.*

Observe that if G_1 and G_2 are abelian, then so is $G_1 \times G_2$. Also, $G_1 \times \{e_2\} = \{(g_1, e_2) : g_1 \in G_1\}$ (where e_2 is the identity in G_2) is a subgroup of $G_1 \times G_2$, which is isomorphic to G_1. Likewise, $\{e_1\} \times G_2 \cong G_2$ is a subgroup of $G_1 \times G_2$. Finally note that $|G_1 \times G_2| = |G_1|\ |G_2|$.

Exercise 7.2. *Prove that $G_1 \times \{e_2\} \cong G_1$ where $G_1 \times \{e_2\} \subset G_1 \times G_2$ and e_2 is the identity element in G_2.*

Consider $G_1 = \{e_1, a_1\}$ with $a_1^2 = e_1$ and $G_2 = \{e_2, a_2\}$ with $a_2^2 = e_2$. That is, $G_1 \cong \mathbb{Z}_2$ and $G_2 \cong \mathbb{Z}_2$. Then $G_1 \times G_2$ has order 4. Hence it must be isomorphic to $\mathbb{Z}_4$ or to V_4. Which one is it? Since all elements of $G_1 \times G_2$ different from (e_1, e_2) are of order 2, this cannot be $\mathbb{Z}_4$, which has at least one element of order 4. Hence it must be V_4. That is, we have found

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

Exercise 7.3. *Prove that $(g_1, g_2) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ where $(g_1, g_2) \neq (e_1, e_2)$ is an element of order two.*

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

Proof. Consider a finite group of even order where $G = \{e, g_1, g_2, \ldots g_{2n-1}\}$ for $n \in \mathbb{Z}$. Suppose that G does not contain any non-identity element of order two and note that such an element is its own inverse element. We may pair up each element and 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 and G contains at least one non-identity element of order two. □

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

Proof. Let $|G| = 6$ then the orders of its elements are 1, 2, 3 or 6. If G contains an element, a, of order 6 then $G = \langle a \rangle \cong \mathbb{Z}_6$. Otherwise if G does not contain any element of order 6, then we know by the previous lemma that it must contain at least one element of order 2. Is it possible that G can consist of just elements of order 2 (besides the identity)? Suppose that $a, b, ab \in G$ are three elements each of order 2, then $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ in which case $\langle a, b \rangle$ with $a^2 = e$, $b^2 = e$ and $(ab)^2 = e$ form a subgroup of order 4, the Klein four-group V_4 in G. However by Lagrange's theorem G with $|G| = 6$ does not have any subgroups of order 4. Hence if G is not isomorphic to $\mathbb{Z}_6$ then it must contain elements of both orders 2 and 3. Let $a^3 = e$ and $b^2 = e$ and construction of the Cayley table leads to two possibilities either $ab = ba$ or $ab = ba^2$. If $ab = ba$ then ab is an element of order 6, which cannot be if G is not isomorphic to $\mathbb{Z}_6$. The other possibility gives $G = \langle a, b \rangle$ with $a^3 = e$, $b^2 = e$ and $ab = ba^2$, meaning that $G \cong S_3$. □

Let us use this theorem in order to study the group $\mathbb{Z}_2 \times \mathbb{Z}_3$. This has order 6. Is it isomorphic to $\mathbb{Z}_6$ or to 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 abelian hence we must have

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

Note how this differs in form from the earlier example (where we found $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V_4$ i.e. $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$). In which situations do we have $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$? The answer is:

Theorem 7.2. $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ *if and only if* p *and* q *are relatively prime (i.e. they do not have prime factors in common).*

Proof. Let $\mathbb{Z}_p = \langle a \rangle$ and $\mathbb{Z}_q = \langle b \rangle$. That is, $a^p = e$ and $b^q = e$, and there are no smaller positive integers such that these are true (here by abuse of language we use the same identity symbol e for both groups).

Consider $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$. We will first show that if p and q are relatively prime then (a, b) has order pq. This will imply that the subgroup $\langle (a, b) \rangle$ of $\mathbb{Z}_p \times \mathbb{Z}_q$ has order $pq = |\mathbb{Z}_p \times \mathbb{Z}_q|$, whence that $\mathbb{Z}_p \times \mathbb{Z}_q = \langle (a, b) \rangle$: it is cyclic. By Theorem 4.3, this will imply that $\mathbb{Z}_p \times \mathbb{Z}_q$ is isomorphic to $\mathbb{Z}_{pq}$.

Let n be the order of the element $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$, i.e. n is the minimal integer such that $(a, b)^n = (e, e)$ (the identity element in $\mathbb{Z}_p \times \mathbb{Z}_q$). Then we must have both $a^n = e$ and $b^n = e$. Hence, $n = rp = tq$ where r and t are positive integers. Hence $r/t = q/p$, and since p and q are relatively prime, we must have $r = q$ and $t = p$. Hence $n = pq$.

For the proof in the opposite direction we must show that if p and q are not relatively prime, then $\mathbb{Z}_p \times \mathbb{Z}_q$ is not isomorphic to $\mathbb{Z}_{pq}$. Let $u \in \mathbb{Z}_p$ and $v \in \mathbb{Z}_q$ be generating elements for $\mathbb{Z}_p$ and $\mathbb{Z}_q$ respectively, and let n be the order of $(u, v) \in \mathbb{Z}_p \times \mathbb{Z}_q$. As above, this implies $n = rp = tq$ with $r/t = q/p$. Since p and q are not relatively prime, they have a factor in common, say $s > 1$. Then we may take $r = q/s$ and $t = p/s$, and we find $n = pq/s < pq$. Therefore the order of the element (u, v) (which have the largest order of any element in $\mathbb{Z}_p \times \mathbb{Z}_q$) is less than pq while $\mathbb{Z}_{pq}$ always has an element of order pq (the generating element). Hence, there is no isomorphism between $\mathbb{Z}_p \times \mathbb{Z}_q$ and $\mathbb{Z}_{pq}$ when p and q are not relatively prime (as isomorphisms preserve the order of elements). $\square$

8. Symmetry Transformations and Dihedral Groups

8.1 Symmetries and Groups

Symmetries are one of the most intuitive ideas in mathematics, from the moment we look in a mirror or first draw a square we are aware of patterns in an image. Even before giving a formal definition of a symmetry we can answer some questions about symmetries and even begin counting them. For example which object is more symmetrical: a circle or a square? Our intuition is that the circle is the more symmetrical. But how does our intuition serve us if we ask whether the triangle or the square is the more symmetrical object? To answer this question we should give a formal definition of a symmetry and also find a way to count the symmetries of these geometric objects.

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

Comment(s). *(On symmetry transformations.)*

1. *An even function $f(x)$ has the property that $f(x) = f(-x)$, it is symmetric under the map $x \to -x$. In $\mathbb{R}^2$ the curve $y = f(x)$ is symmetric under a reflection in the y-axis. An odd function satisfies $g(x) = -g(-x)$ and in $\mathbb{R}^2$ the curve $y = g(x)$ is not symmetric under reflection in the y-axis, on the other hand it is symmetric under another transformation of $\mathbb{R}^2$ (which one?)*

2. *Any geometric shape may be considered as a set of points, e.g. a unit square can be described as the set of points $\{(0, y), (x, 0), (1, y), (x, 1) : x, y \in [0, 1]\}$, the unit circle at the origin is the set of points (x, y) satisfying $x^2 + y^2 = 1$ and so on.*

3. *Suppose we were to define a square by its four vertices $\{A, B, C, D\}$, then a symmetry transformation may move these vertices around e.g. $A \to B$, $B \to C$, $C \to D$ and $D \to A$ (and hence move all the points on the square about) but $\{A, B, C, D\} \to \{B, C, D, A\} = \{A, B, C, D\}$ as there is no order on a set. A non-trivial symmetry transformation is a map of set to itself.*

4. *Every group is a set G together with a map that maps the set G to itself, hence every group action encodes a symmetry transformation of G. Equivalently we can commence with a set and by identifying its symmetry transformations we can construct the associated group.*

5. *By encoding symmetry transformations as a group G we have a natural way to count the number of symmetries, it is just the order of the group $|G|$, so we have a canonical way to answer the question of whether the triangle or the square is the more symmetric object and further we will be able to say that the circle has an infinite number of symmetry transformations.*

8.2 Isometries of the Euclidean Plane

Let us consider the natural transformations of the Euclidean plane: translations, rotations and reflections. Each of these transformations is a symmetry of the Euclidean plane, but they are also special symmetries as they are the symmetry transformations which preserve distance between pairs of points on the 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 $f(x_2) = y_2$.

We will be interested in the Euclidean plane and so will consider the isometries when $X = Y = \mathbb{R}^2$ and the distance function is the Euclidean inner product: $D_{\mathbb{R}^2}(\boldsymbol{x}, \boldsymbol{y}) = |\boldsymbol{y} - \boldsymbol{x}|$. The isometries of the Euclidean plane are also called the Euclidean transformations. The reflections and rotations are the only Euclidean transformations of the Euclidean plane, we will prove this statement later in the course when we construct the Euclidean group. Now we will investigate the Euclidean transformations of simple geometric objects.

Consider the subset of the plane formed by a circle centred at the origin and of radius 1:

$$\{(x, y) : x^2 + y^2 = 1\}. \tag{8.1}$$

What are its isometries? The only Euclidean transformations that preserve this circle are the rotations with respect to the origin, and the reflections with respect to any axis passing through the origin. We can describe these by matrices, acting on the coordinates $\begin{pmatrix} x \\ y \end{pmatrix}$ simply by matrix multiplication. Rotations are

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

We can also find a matrix representation for the reflections. There are many reflections and one of them is the reflection in the x-axis (i.e. mapping $x \to x$ and $y \to -y$):

$$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Reflections through another axis, at angle θ to the x-axis, denoted $B(\theta)$ can be obtained by combining $A(\theta)$ and B. Geometrically, if we want to construct a reflection through the axis that is at angle θ, we just need to first rotate the angle-θ axis to the x axis by a rotation $A_{-\theta}$, then do a reflection, then rotate back by an angle θ. That is,

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

Of course, here we only need to take $\theta \in [0, \pi)$, because if we rotate an axis by π we get again the same axis. Hence the set of all symmetry transformations is $\{A(\theta) : \theta \in [0, 2\pi)\} \cup \{B(\theta) : \theta \in [0, \pi)\}$.

Combinations of these transformation also give a Euclidean transformation that preserves the circle, hence under matrix multiplication this set satisfies the closure axiom of a group. The identity transformation is $A(0)$ (rotation by angle 0) is one of the symmetry transformations of the circle. Further all inverse transformations are included in this set. Hence the set of symmetry transformations of the circle form a group. It is, in general, very natural to interpret group elements as transformations, and the study of symmetries, transformations that preserve sets, equations, etc., is the study of the groups (and their representations) formed by such transformations.

Closure, identity and inverses can be verified explicitly here using the matrices and matrix multiplication. In general, a multiple rotation is equivalent to a single rotation by the sum of the angles defining the multiple rotations, and two reflections give the identity:

$$A(\theta)A(\theta') = A(\theta + \theta'), \quad A(2\pi) = I, \quad B^2 = I \tag{8.2}$$

Exercise 8.1. *Check these statement by carrying out the matrix multiplications.*

Further one can confirm the relation

$$A(\theta)B = BA(-\theta). \tag{8.3}$$

(Observe how similar these are to the relations in S_3: $a^3 = e$, $b^2 = e$ and $ab = ba^2 = ba^{-1}$.) Hence, we may express $B(\theta)$ as

$$B(\theta) = A(2\theta)B. \tag{8.4}$$

Using (8.2), (8.3) and (8.4), the product of any two transformations can be re-written as another transformation confirming that we have closure.

In order to check explicitly that some matrix multiplication gives rise to a symmetry of the subset (8.1), we may proceed by starting with the expression for the transformed subset, and then make a change of variable in order to recover the original subset. Notice that $A(\theta)$, $B(\theta)$ all are orthogonal matrices, i.e. matrices M satisfying $M^TM = MM^T = I$. Let us then consider such an orthogonal matrix for the transformation:

$$\begin{aligned}
\left\{M\begin{pmatrix} x \\ y \end{pmatrix} : x^2+y^2=1\right\} &= \left\{M\begin{pmatrix} x \\ y \end{pmatrix} : \begin{pmatrix} x \\ y \end{pmatrix}^T\begin{pmatrix} x \\ y \end{pmatrix}=1\right\} \\
&= \left\{\begin{pmatrix} x' \\ y' \end{pmatrix} : \left(M^T\begin{pmatrix} x' \\ y' \end{pmatrix}\right)^T\left(M^T\begin{pmatrix} x' \\ y' \end{pmatrix}\right)=1\right\} \\
&= \left\{\begin{pmatrix} x' \\ y' \end{pmatrix} : \begin{pmatrix} x' \\ y' \end{pmatrix}^T MM^T\begin{pmatrix} x' \\ y' \end{pmatrix}=1\right\} \\
&= \left\{\begin{pmatrix} x' \\ y' \end{pmatrix} : \begin{pmatrix} x' \\ y' \end{pmatrix}^T\begin{pmatrix} x' \\ y' \end{pmatrix}=1\right\} \\
&= \left\{\begin{pmatrix} x' \\ y' \end{pmatrix} : (x')^2+(y')^2=1\right\}
\end{aligned}$$

Hence we get back to the set (8.1). The group we have been considering is called the special orthogonal group $SO(2)$ - we will discuss this group in detail in later chapter. It is a complicated group, it contains an infinite number of group elements (there are elements $A(\theta)$ and $B(\theta)$ for every $\theta \in \mathbb{R}$). It is an example of a Lie group. It is sensible for us to consider objects which have less symmetry than the circle and construct their symmetry groups. Let us consider, instead of the circle, the polygons.

Definition 8.3. *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*

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

straight lines, is called the dihedral group D_n.

Comment(s). *(On the dihedral group and polygons)*

1. *D_n is the symmetry group of the regular polygon P_n.*
2. *Note that the case $n = 2$ does not quite form a polygon - P_2 is just a line segment. However it fits into the considerations below very well.*

We will consider the cases $n = 2$, $n = 3$ and the class $n \geq 4$ and in each case we will identify the symmetries of P_n in terms of rotations and reflections of the Euclidean plane.

- $n = 2$. From geometric considerations, the symmetries of the segment are the rotations by angle 0 (the identity) and π, as well as the reflections with respect to axes at angles 0 and $\pi/2$, i.e. the x and y axes. These are the matrices, in the notation $A(\theta)$ (rotation by an angle θ) and $B(\theta)$ (reflection with respect to the axis at angle θ from the x axis, with $B(0) = B$) introduced above:

$$A(0) = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A(\pi) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$B(0) = B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B(\pi/2) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

To show that, e.g., $A(\pi)$ is a symmetry, we may proceed as follows: the segment is described by $\{(x, y) : y = 0,\ -1 < x < 1\}$, and the transformed segment is

$$\begin{aligned} \left\{A(\pi)\begin{pmatrix} x \\ y \end{pmatrix} : y = 0,\ -1 < x < 1\right\} &= \left\{\begin{pmatrix} -x \\ -y \end{pmatrix} : y = 0,\ -1 < x < 1\right\} \\ &= \left\{\begin{pmatrix} x' \\ y' \end{pmatrix} : -y' = 0,\ -1 < -x' < 1\right\} \\ &= \left\{\begin{pmatrix} x' \\ y' \end{pmatrix} : y' = 0,\ -1 < x' < 1\right\} \end{aligned}$$

where we have made the change of variable $x' = -x$ and $y' = -y$, and have used $-x' < 1 \Rightarrow x' > -1$ and $-1 < -x' \Rightarrow x' < 1$. We notice that these are the same matrices as those of the Klein four-group V_4, so we have $D_2 \cong V_4$. We know that $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Can we interpret the $\mathbb{Z}_2$ factors in the symmetry transformations of P_2? Yes. Consider A_π and B. They satisfy $A(\pi)^2 = A(2\pi) = I$ and $B^2 = I$. Also, $A(\pi)B = BA(\pi)$. These are the relations describing the group V_4: the set $\{I, A(\pi), B, A(\pi)B\}$ have the multiplication law of the group V_4. Also, there are at least two $\mathbb{Z}_2$ subgroups: $\{I, A(\pi)\}$ (identity and rotation by π) and $\{I, B\}$ (the identity and the reflection with respect to the x-axis). The direct product $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a way of putting these two subgroups together into one whole symmetry group of a single mathematical object.

- $n = 3$. From geometric considerations, the symmetries are the identity, the rotations $A(2\pi/3)$, $A(4\pi/3)$, and the reflections B, $B(\pi/3)$ and $B(2\pi/3)$. Note that the angles the axes of reflection make to the x-axis are half of those of the rotation symmetries. This is a general fact for the dihedral groups. Note also that there are 3 rotations and 3 reflections in D_3, a pattern which will also generalise to other dihedral groups. Hence $|D_3| = 6$. We know by Theorem 7.1 the group can only be S_3 or $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Which group is it? A simple check is that the matrices don't all commute; for instance, a rotation followed by a reflection gives something different than the same reflection followed by the same rotation. So we must have S_3. More precisely, we have $A(2\pi/3)^3 = I$ and $B^2 = I$, as well as $A(2\pi/3)B = BA(2\pi/3)^2$ and $A(2\pi/3)^2B = BA(2\pi/3)$. These are indeed the relations describing the group S_3. Hence, we have $D_3 \cong S_3$. We note that P_3 is an equilateral triangle, and that the rotations just cyclically permute the three vertices, and the reflection B exchanges two vertices. These are indeed what the elements of S_3 do to the 3 elements $1, 2, 3$ and one can formally construct the isomorphism between S_3 and D_3 to show that $D_3 \cong S_3$.

Exercise 8.2. *Prove that $D_3 \cong S_3$.*

- In general, for $n \geq 3$, we can set $e = I$, $a = A(2\pi/n)$ and $b = B$, and we have $a^n = e$, $b^2 = e$ and $a^k b = ba^{-k}$ for $k = 1, 2, \ldots, n-1$ (the cases $k = 1$ and $k = n-1$ are the same, etc.). The set of group elements generated by these symbols under these relations is $\{e, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$. This is the group D_n, and it has order $2n$.

Exercise 8.3. *Is D_n isomorphic to S_n for $n > 3$?*

9. Conjugation, Normal Subgroups, Quotient Groups

9.1 Conjugation

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

Conjugation is a way of relating similar transformations. Consider the permutation (123) in the symmetric group S_3. If we swapped the labels of the elements $2 \leftrightarrow 3$ we would find another 3-cycle permutation: (132). The two permutations are both 3-cycles and in this sense are similar transformations. We can carry out the swap $2 \leftrightarrow 3$ using elements of S_3 as follows:

$$(23)(123)(32) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132).$$

The operation (23)(123)(32) is conjugation of (123) with $g = (23)$. As every finite group G is made up of some set of permutations in the symmetric group $S_{|G|}$ then the usefulness of conjugation within the symmetric group is inherited by its subgroup G. The bottom line is that conjugation is a means of relating similar group elements.

Theorem 9.1. *The conjugacy relation is an equivalence relation.*

Proof. We check the properties of an equivalence relation for conjugation.

- Reflexivity: a is conjugate to itself as $a = eae^{-1}$ and $e \in G$.
- Symmetry: If a is conjugate to b, then $a = gbg^{-1}$ (for some $g \in G$) $\Rightarrow b = g^{-1}ag = g^{-1}a(g^{-1})^{-1}$ hence b is conjugate to a.
- Transitivity: If a is conjugate to b and b is conjugate to c, then $a = gbg^{-1}$ and $b = g'c(g')^{-1}$ (for some $g, g' \in G$), hence $a = gg'c(g')^{-1}g^{-1} = gg'c(gg')^{-1}$ and so a is conjugate to c.

□

Hence, the group G is divided into conjugacy classes, $[a]_C = \{gag^{-1} : g \in G\}$. By Theorem 5.1 (applied to general equivalence classes), two such conjugacy classes are either disjoint or identical. The conjugacy classes cover the whole group because $a \in [a]_C$ for every $a \in G$, i.e. $\cup_{a\in G}[a]_C \subset \cup_{a\in G}\{a\} = G$. Hence conjugacy classes form a partition of G. Contrary to cosets, however, this is not an equipartition.

Comment(s). *(On conjugacy classes.)*

- $[e]_C = \{e\}$. *Hence no other class is a subgroup (because* $e \notin [a]_C$ *for any* $a \neq e$*).*

- *All elements of a conjugacy class have the same order. Indeed let* b *be an element of* $[a]_C$*. Then* $b = gag^{-1}$ *for some* $g \in G$*. Hence,* $b^n = (gag^{-1})^n = gag^{-1}\ gag^{-1}\ \cdots\ gag^{-1}$ *(*n *factors)* $= ga^ng^{-1}$ *(using* $g^{-1}g = e$*). Now if* k *is the order of* b *then* $b^k = e$ *and so* $a^k = e$*. Further suppose there exists* $k' < k$ *such that* $a^{k'} = e$*, then* $b^{k'} = ga^{k'}g^{-1} = geg^{-1} = e$ *contradicting the assumption that the order of* b *is* k *(as* $k' < k$*) hence no such* k' *exists. A similar argument holds in the other direction (i.e. assuming the order of* a *is* k *to show that it implies the same order for* b*). Hence* a *and* b *have the same order.*

- *If* G *is abelian, then* $[a]_C = \{a\}$ *for all* $a \in G$*.*

Theorem 9.2. *On any subset* $H \subset G$*, the conjugation map* $M : H \mapsto gHg^{-1},\ h \mapsto ghg^{-1}$ *associated to* $g \in G$ *is bijective.*

Proof. Injective: if $ghg^{-1} = gh'g^{-1}$ then, by pre/post-multiplying by g^{-1} / g, we have $h = h'$; surjective: any $b \in gHg^{-1}$ can be written as $b = ghg^{-1}$ for some $h \in H$, so $b = M(h)$. □

9.2 Normal subgroups.

Definition 9.1. *A subgroup* H *is called normal or invariant if* $gHg^{-1} \subset H$ *for all* $g \in G$*.*

Comment(s). *(On normal subgroups.)*

1. *Notation:* $gHg^{-1} = \{ghg^{-1} : h \in H\}$*). That is,* H *is normal if for every* $h \in H$ *and every* $g \in G$*, we have* $ghg^{-1} \in H$*.*

2. *An immediate consequence is that if* H *is normal, then* $gHg^{-1} = H$ *for all* $g \in G$*. This follows from Theorem 9.2. Let* M *be the conjugation map of Theorem 9.2, by normality of* H*, we have* $M(H) \subset H$*, and by bijectivity of* M*, we have* $|M(H)| = |H|$*, hence* $M(H) = H$*.*

3. *Let H be a normal subgroup. If $h \in H$ then $[h] \subset H$. That is, H is composed of entire conjugacy classes. In fact: a subgroup is normal if and only if the subgroup is the union of conjugacy classes.*

4. *$\{e\}$ is a (trivial) normal subgroup.*

5. *Every subgroup of an abelian group is normal.*

Exercise 9.1. *Prove that every subgroup of an abelian group is indeed normal.*

Definition 9.2. *A group is simple if it has no proper normal subgroup. A group is semi-simple if it has no proper abelian normal subgroup.*

Definition 9.3. *The centre $Z(G)$ of a group G is the set of all elements which commute with all elements of G:*

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

Theorem 9.3. *The centre $Z(G)$ of a group is a normal subgroup.*

Proof. We must first show that $Z(G)$ is a subgroup and second that it is a normal subgroup. It is a subgroup as it satisfies the group axioms:

- 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 elements: let $a \in Z(G)$ and $g \in G$ then $ag^{-1} = g^{-1}a$ hence $ga^{-1} = a^{-1}g$ hence $a^{-1} \in Z(G)$.
- Associativity: $Z(G)$ has the same group multiplication rule as G, which is associative as G is a group by construction.

It is normal as it is abelian, i.e. for $a \in Z(G)$ and $g \in G$ then $gag^{-1} = gg^{-1}a = a \in Z(G)$. □

Observe that, by the above definitions and by Theorem 9.2, if G is simple, then $Z(G) = \{e\}$ or $Z(G) = G$.

9.3 Quotients

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

Definition 9.4. *The quotient $G/H = \{aH : a \in G\}$ is the set of all left-cosets. The quotient $H\backslash G = \{Ha : a \in G\}$ is the set of all right-cosets.*

We will focus our discussion on G/H (the set of left-cosets), but a similar discussion holds for $H\backslash G$.

We will first define a multiplication law on subsets of a group:

Definition 9.5. *Given two subsets A and B of G, the multiplication of set A by set B is defined by element-wise multiplication, $AB := \{ab : a \in A, b \in B\}$.*

Theorem 9.4. *If H is normal, then the quotient G/H, with the above multiplication law on subsets, is a group.*

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

- Closure: We have $(g_1H)(g_2H) = g_1Hg_2H = g_1g_2g_2^{-1}Hg_2H = g_1g_2HH$ where we used $g_2^{-1}Hg_2 = H$, which holds because H is a normal subgroup. Since H is a subgroup, we have $HH \subset H$. But also since $e \in H$, we have that $HH \supset H$. Hence $HH = H$, and we find $(g_1H)(g_2H) = g_1g_2H$. That is, we have closure with the multiplication law
$$(g_1H)(g_2H) = g_1g_2H. \tag{9.1}$$
- Associativity: This follows immediately from associativity of G and the relation (9.1).
- Identity: Similarly it follows that $eH = H$ is an identity.
- Inverse: Similarly it follows that $g^{-1}H$ is the inverse of gH under the multiplication law (9.1).

□

We call G/H the left-quotient group of G with respect to H.

Example 9.1. *Take $S_3 = \{e, a, a^2, b, ab, a^2b\}$ with $a^3 = e$, $b^2 = e$ and $a^2b = ba$. Now $H = \{e, a, a^2\}$ is a normal subgroup as since as $H = \langle a\rangle$ it is a subgroup, and it is normal $gag^{-1} \in H$ for $g \in S_3$. We must explicitly check the statement that it is normal: it is evident that for $g = e$, $g = a$, and $g = a^2$ we have $geg^{-1} \in H$, $gag^{-1} \in H$, $ga^2g^{-1} \in H$ but it is less obvious for $g = b$, $g = ab$ and $g = a^2b$ and we now check these explicitly (using $ab = ba^2$ as well as the defining relations for S_3)*

- *For $g = b$, $g^{-1} = b$ so that $gag^{-1} = bab = a^2b^2 = a^2 \in H$ and $ga^2g^{-1} = ba^2b = ab^2 = a \in H$.*
- *For $g = ab$, $g^{-1} = (ab)^{-1} = b^{-1}a^{-1} = ba^2$ so that $gag^{-1} = (ab)a(ba^2) = a(a^2b)(ba^2) = a^3b^2a^2 = a^2 \in H$ and $ga^2g^{-1} = (ab)a^2(ba^2) = a^2b^2a^2 = a \in H$.*

- *For* $g = a^2b$, $g^{-1} = (a^2b)^{-1} = b^{-1}(a^2)^{-1} = ba$ *so that* $gag^{-1} = (a^2b)a(ba) = (a^2b)(ba^2)a = a^2b^2a^3 = a^2 \in H$ *and* $ga^2g^{-1} = (a^2b)a^2(ba) = a^3b^2a = a \in H$.

Hence H *is normal.*

Interestingly, we also obtain from these calculations the conjugacy classes of a *and* a^2*. We have found* $[a]_C = \{a, a^2\}$ *and* $[a^2]_C = \{a, a^2\}$*. Along with* $[e]_C = \{e\}$*, we see indeed that* $H = [e]_C \cup [a]_C$ *so it contains whole conjugacy classes.*

By previous examples and by Lagrange's theorem we know that there are two left-cosets with respect to H*: these are* H *and* $bH = \{b, ab, a^2b\}$*. Hence,* S_3/H *has two elements,* H *and* bH*. Explicitly multiplying these subsets we find:*

$$HH = H, \quad H\,bH = bH\,H = bH, \quad bH\,bH = H.$$

Indeed this forms a group and is in agreement with the relation (9.1) *(using* $b^2 = e$*). In the end, we find that the multiplication law is that of* $\mathbb{Z}_2$*, i.e.*

$$S_3/H \cong \mathbb{Z}_2 \tag{9.2}$$

Explicitly, the isomorphism that maps S_3/H *onto* $\mathbb{Z}_2 = \{0, 1\}$ *is* $\phi(H) = 0$, $\phi(bH) = 1$.

10. Kernel, Image and the Homomorphism Theorem

Definition 10.1. *Let ϕ be a homomorphism of G_1 onto G_2. Then the kernel of ϕ_1 is*

$$\ker\phi_1 \; = \{g \in G_1 : \phi(g) = e_2\}$$

where e_2 is the identity element of G_2.

Observe that $e_1 \in \ker\phi_1$ due to part (i) of Theorem 4.1.

Theorem 10.1. *A homomorphism $\phi : G \to G'$ is an isomorphism if and only if it is onto and* $\ker\phi = \{e\}$*.*

Proof. We must prove the theorem in two directions: (In one direction ϕ is an isomorphism $\Rightarrow$ ϕ is onto and $ker\phi = \{e\}$): If ϕ is an isomorphism, then ϕ is bijective, in particular injective. We know that $\phi(e) = e'$ (by Theorem 4.1). If $g \in \ker\phi$ then also $\phi(g) = e'$. Injectivity implies $g = e$. Hence $\ker\phi = \{e\}$.
(In the other direction ϕ is onto and $ker\phi = \{e\} \Rightarrow \phi$ is an isomorphism): if $\ker\phi = \{e\}$ and ϕ is onto, then we only need to prove injectivity. If $\phi(g_1) = \phi(g_2)$ then $\phi(g_1)\phi(g_2)^{-1} = e'$ hence $\phi(g_1)\phi(g_2^{-1}) = e'$ using part (ii) of Theorem 4.1. Therefore $\phi(g_1 g_2^{-1}) = e'$ (using homomorphism property) hence $g_1 g_2^{-1} = e$ (using $\ker\phi = \{e\}$). Hence $g_1 = g_2$, and we have injectivity.

□

In the following, we will often use Theorem 4.1 without mentioning it.

Theorem 10.2. *The kernel is a normal subgroup.*

Proof. Let $\phi : G \to G'$ and $H = \ker\phi \subset G$. We first show that H is a subgroup:

- Closure: if $h_1, h_2 \in H$ then $\phi(h_1 h_2) = \phi(h_1)\phi(h_2) = e'e' = e'$ hence $h_1 h_2 \in H$;

- Associativity: derived from the associativity of G;
- Identity: $\phi(e) = e'$ hence $e \in H$;
- Inverses: if $h \in H$ then $\phi(h^{-1}) = \phi(h)^{-1} = e'^{-1} = e'$ hence $h^{-1} \in H$.

Hence H is a subgroup. Now we show that the kernel is a normal subgroup: if $h \in H$ and $g \in G$ then $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = e'$ hence $ghg^{-1} \in H$. Therefore H is a normal subgroup. □

Theorem 10.3. *The image* $\mathrm{Im}(\phi)$ *of a homomorphism* $\phi : G_1 \to G_2$ *is a subgroup of* G_2.

Proof. Let $g_2, g_2' \in \mathrm{Im}(\phi) \subset G_2$. That is, $g_2 = \phi(g_1)$, $g_2' = \phi(g_1')$ with $g_1, g_1' \in G_1$.

- Closure: $g_2g_2' = \phi(g_1)\phi(g_1') = \phi(g_1g_1') \in \mathrm{Im}(\phi)$.
- Associativity: is derived from the associativity of G_2 as $\mathrm{Im}(\phi) \subset G_2$;
- Identity: $\phi(e_1) = e_2$, hence $e_2 \in \mathrm{Im}(\phi)$.
- Inverses: $g_2^{-1} = \phi(g_1)^{-1} = \phi(g_1^{-1}) \in \mathrm{Im}(\phi)$.

□

10.1 The Homomorphism Theorem

We will illustrate the theorem first through two examples.

Example 10.1. *Let* $\mathbb{R}^*$ *be the nonzero reals. This is a group under multiplication of real numbers (*$e = 1$, $x^{-1} = 1/x$*). The subgroup* $\{1, -1\} \in \mathbb{R}^*$ *is isomorphic to* $\mathbb{Z}_2$*. Let* $\mathbb{R}^+$ *be the group of positive real numbers (it is a normal subgroup of* $\mathbb{R}^*$*, but this doesn't matter). Define*

$$\phi : \mathbb{R}^* \to \mathbb{R}^+, \quad \phi(x) = |x|. \tag{10.1}$$

This is a homomorphism onto $\mathbb{R}^+$*:* $\phi(xx') = |xx'| = |x|\,|x'| = \phi(x)\phi(x')$*. Its kernel is* $\ker\phi = \{x \in \mathbb{R}^* : |x| = 1\} = \{1, -1\} = \mathbb{Z}_2$*. Hence* $\mathbb{Z}_2$ *is a normal subgroup of* $\mathbb{R}^*$*. Further, let us calculate* $\mathbb{R}^*/\mathbb{Z}_2$*. This is the set of all cosets of the form* $x\mathbb{Z}_2$ *for* $x \in \mathbb{R}^*$*. This can be simplified:* $\{x\mathbb{Z}_2 : x \in \mathbb{R}^*\} = \{\{x, -x\} : x \in \mathbb{R}^*\} = \{\{x, -x\} : x \in \mathbb{R}^+\}$*. That is, it is the set of pairs of number and its negative, and each pair can be completely characterised by a positive real number. As we know these pairs form a group, the quotient group, under element-wise multiplication of sets:* $\{x, -x\}\{x', -x'\} = \{xx', -xx'\}$*. What is this group isomorphic to, whose elements are parameterised by* $\mathbb{R}^+$*?*

There is an isomorphism between $\mathbb{R}^*/\mathbb{Z}_2$ and the group $\mathbb{R}^+$ itself. Indeed, define $\psi : \mathbb{R}^*/\mathbb{Z}_2 \to \mathbb{R}^+$ as the bijective map $\psi(\{x,-x\}) = x$ (for $x \in \mathbb{R}^+$). It is clearly onto, and it is injective because given a value of $x > 0$, there is a unique pair $\{x,-x\}$. Also, it is a homomorphism: for any $x, x' \in \mathbb{R}^+$, we have $\psi(\{x,-x\}\{x',-x'\}) = \psi(\{xx',-xx'\}) = xx' = \psi(\{x,-x\})\,\psi(\{x',-x'\})$. Hence, we have found that $\mathbb{R}^*/\mathbb{Z}_2 \cong \mathbb{R}^+$, that is,

$$\mathbb{R}^*/\mathrm{ker}\phi \cong \mathrm{Im}\phi.$$

Example 10.2. *Consider the example of S_3 and $H = \{e, a, a^2\}$ discussed at the end of Section 9. We have the following homomorphism: $\phi : S_3 = \{e, a, a^2, b, ab, a^2b\} \to \mathbb{Z}_2 = \{e, b\}$ given by $\phi(a^n) = e$ and $\phi(a^n b) = b$. This is a homomorphism on to $\mathbb{Z}_2$, which we check explicitly: $\phi(a^n a^m) = \phi(a^{n+m}) = e = \phi(a^n)\phi(a^m)$, $\phi(a^n b\, a^m b) = \phi(a^{n-m}b^2) = \phi(a^{n-m}) = e = b^2 = \phi(a^n b)\phi(a^m b)$, $\phi(a^n b\, a^m) = \phi(a^{n-m}b) = b = be = \phi(a^n b)\phi(a^m)$, $\phi(a^n a^m b) = \phi(a^{n+m}b) = b = \phi(a^n)\phi(a^m b)$. Also, it is clear from the definition of ϕ that $\mathrm{ker}\phi = H$. Recall equation (9.2). This is then re-written as $S_3/\mathrm{ker}\phi \cong \mathrm{Im}\phi$.*

Theorem 10.4. *(The homomorphism theorem) Let G and G' be groups, and $\phi : G \to G'$ be a homomorphism. Then, $G/\mathrm{ker}\phi \cong \mathrm{Im}\phi$.*

Proof. Let $H = \mathrm{ker}\phi$ (this is a normal subgroup of G) and $\tilde{G} = G/H$. Let us first find a homomorphism $\tilde{\phi} : \tilde{G} \to \mathrm{Im}\phi$. We define the map $\tilde{\phi}$ as $\tilde{\phi}(gH) = \phi(gH) = \{\phi(gh) : h \in H\}$. This seems a priori multi-valued, but let us show that it is in fact single-valued. Indeed, $\phi(gh) = \phi(g)\phi(h) = \phi(g)$ for all $h \in H$ because H is the kernel of ϕ. Hence $\tilde{\phi}(gH) = \phi(g)$, which is single valued. We then show that $\tilde{\phi}$ is a homomorphism: $\tilde{\phi}(gHg'H) = \tilde{\phi}(gg'H) = \phi(gg') = \phi(g)\phi(g') = \tilde{\phi}(gH)\tilde{\phi}(g'H)$.

Second, we show that $\tilde{\phi}$ is bijective. It is clearly surjective as $\mathrm{Im}\tilde{\phi} = \{\tilde{\phi}(gH) : g \in G\} = \{\phi(g) : g \in G\} = \mathrm{Im}\phi$. Hence we only need to show injectivity. Suppose $\tilde{\phi}(gH) = \tilde{\phi}(g'H)$. Then $\phi(g) = \phi(g')$. Hence $e = \phi(g)^{-1}\phi(g') = \phi(g^{-1})\phi(g') = \phi(g^{-1}g')$, and therefore $g^{-1}g' \in H$, so that $g' = gh$ for some $h \in H$. That is, $g \sim g'$ under the left-coset equivalence relation, so that $gH = g'H$. □

Example 10.3. *Let G be the group of N-by-N matrices with non-zero determinant and real entries (denoted $GL(N,\mathbb{R})$) and let $\phi = \det$, the determinant, so $\phi : GL(N,\mathbb{R}) \to \mathbb{R}^*$ and is a homomorphism (as for $A, B \in GL(N,\mathbb{R})$ we have $\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B)$) then ker$\phi := \{M \in GL(N,\mathbb{R}) : \det M = 1\} = SL(N,\mathbb{R})$ the special linear transformations, the group of N-by-N matrices with real entries and unit determinant. The homomorphism theorem then implies that $GL(N,\mathbb{R})/SL(N,\mathbb{R}) \cong \mathbb{R}^*$.*

Theorem 10.5. *Given a group G and a normal subgroup H, there exists a homomorphism $\phi : G \to G/H$ (onto) such that $\mathrm{ker}\phi = H$.*

Proof. If $g \in G$, let $\phi(g) = gH$. This is a homomorphism: $\phi(gg') = gg'H = gHg'H = \phi(g)\phi(g')$. Its kernel is $\ker\phi = \{g \in G : gH = H\} = \{g \in G : g \sim e\} = eH = H$. □

Corollary 10.1.1. *Simple groups, having no non-trivial normal subgroups, admit only trivial homomorphisms.*

Example 10.4. *Consider the groups*

$$K_2 = \left\{ \begin{pmatrix} \lambda^{-1} & 0 \\ \mu & \lambda \end{pmatrix} : \mu \in \mathbb{C}, \lambda \in \mathbb{C}^* \right\}$$

$$L_2 = \left\{ \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in \mathbb{C} \right\}$$

We can check that K_2 is a group, and that L_2 is a normal subgroup of K_2.

K_2 is a group:

- *Closure:*
$$\begin{pmatrix} \lambda^{-1} & 0 \\ \mu & \lambda \end{pmatrix} \begin{pmatrix} \tilde{\lambda}^{-1} & 0 \\ \tilde{\mu} & \tilde{\lambda} \end{pmatrix} = \begin{pmatrix} (\lambda\tilde{\lambda})^{-1} & 0 \\ \mu\tilde{\lambda}^{-1} + \lambda\tilde{\mu} & \lambda\tilde{\lambda} \end{pmatrix}$$
and $\lambda\tilde{\lambda} \in \mathbb{C}^*$, $\mu\tilde{\lambda}^{-1} + \lambda\tilde{\mu} \in \mathbb{C}$.

- *Associativity: immediate from matrix multiplication.*

- *Identity: choose $\lambda = 1 \in \mathbb{C}^*$ and $\mu = 0 \in \mathbb{C}$.*

- *Inverse: using the formula for the inverse of a two-by-two matrix,*
$$\begin{pmatrix} \lambda^{-1} & 0 \\ \mu & \lambda \end{pmatrix}^{-1} = \begin{pmatrix} \lambda & 0 \\ -\mu & \lambda^{-1} \end{pmatrix}$$
and $\lambda^{-1} \in \mathbb{C}^*$ and $-\mu \in \mathbb{C}$.

L_2 is a subgroup: Set $\lambda = 1$ in the considerations above for K_2, this is a subset that is preserved under multiplication (check multiplication law above), that contains the identity ($\mu = 0$) and that contains the inverse of every element (check from by setting $\lambda = 1$ in the inverse above for K_2).

L_2 is a normal subgroup: under the multiplication rule, elements of the diagonal get multiplied directly. Hence, with element $g = \begin{pmatrix} \lambda^{-1} & 0 \\ \mu & \lambda \end{pmatrix} \in K_2$ and $h = \begin{pmatrix} 1 & 0 \\ \tilde{\mu} & 1 \end{pmatrix} \in L_2$, we have

that ghg^{-1} is a matrix with on the diagonal $\lambda \cdot 1 \cdot \lambda^{-1} = 1$ and $\lambda^{-1} \cdot 1 \cdot \lambda = 1$, hence matrix of the form $\begin{pmatrix} 1 & 0 \\ \tilde{\tilde{\mu}} & 1 \end{pmatrix} \in L_2$.

So, we can form the quotient group K_2/L_2: this is the group of left-cosets, under element-wise multiplication of left-cosets. The set of left cosets is

$$\begin{aligned}
\{gL_2 : g \in K_2\} &= \left\{ \begin{pmatrix} \lambda^{-1} & 0 \\ \mu & \lambda \end{pmatrix} \left\{ \begin{pmatrix} 1 & 0 \\ \tilde{\mu} & 1 \end{pmatrix} : \tilde{\mu} \in \mathbb{C} \right\} : \mu, \lambda \in \mathbb{C}; \lambda \neq 0 \right\} \\
&= \left\{ \left\{ \begin{pmatrix} \lambda^{-1} & 0 \\ \mu + \lambda\tilde{\mu} & \lambda \end{pmatrix} : \tilde{\mu} \in \mathbb{C} \right\} : \mu, \lambda \in \mathbb{C}; \lambda \neq 0 \right\} \\
&= \left\{ \left\{ \begin{pmatrix} \lambda^{-1} & 0 \\ \tilde{\mu}' & \lambda \end{pmatrix} : \tilde{\mu}' \in \mathbb{C} \right\} : \mu, \lambda \in \mathbb{C}; \lambda \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} \lambda^{-1} & 0 \\ \mathbb{C} & \lambda \end{pmatrix} : \lambda \in \mathbb{C}; \lambda \neq 0 \right\}
\end{aligned}$$

where in the third step, we changed variable to $\tilde{\mu}' = \mu + \lambda\tilde{\mu}$ which preserves $\mathbb{C}$ because $\lambda \neq 0$, i.e. $\{\mu + \lambda\tilde{\mu} : \tilde{\mu} \in \mathbb{C}\} = \mathbb{C}$. That is, a left-coset is a subset $\begin{pmatrix} \lambda^{-1} & 0 \\ \mathbb{C} & \lambda \end{pmatrix}$.

The multiplication law is

$$\begin{pmatrix} \lambda^{-1} & 0 \\ \mathbb{C} & \lambda \end{pmatrix} \begin{pmatrix} \tilde{\lambda}^{-1} & 0 \\ \mathbb{C} & \tilde{\lambda} \end{pmatrix} = \begin{pmatrix} (\lambda\tilde{\lambda})^{-1} & 0 \\ \mathbb{C}\tilde{\lambda}^{-1} + \lambda\mathbb{C} & \lambda\tilde{\lambda} \end{pmatrix} = \begin{pmatrix} (\lambda\tilde{\lambda})^{-1} & 0 \\ \mathbb{C} & \lambda\tilde{\lambda} \end{pmatrix}$$

hence clearly the identity in the quotient group is

$$\begin{pmatrix} 1 & 0 \\ \mathbb{C} & 1 \end{pmatrix} = L_2$$

There exists a bijective map $\phi : K_2/L_2 \to \mathbb{C}^* = \{\lambda \in \mathbb{C} : \lambda \neq 0\}$, given by

$$\phi\left(\begin{pmatrix} \lambda^{-1} & 0 \\ \mathbb{C} & \lambda \end{pmatrix}\right) = \lambda$$

This is bijective. Indeed, it is surjective: given $\lambda \in \mathbb{C}^*$, there is the element $\begin{pmatrix} \lambda^{-1} & 0 \\ \mathbb{C} & \lambda \end{pmatrix}$ that maps to it; and it is injective: if both $\begin{pmatrix} \lambda_1^{-1} & 0 \\ \mathbb{C} & \lambda_1 \end{pmatrix}$ and $\begin{pmatrix} \lambda_2^{-1} & 0 \\ \mathbb{C} & \lambda_2 \end{pmatrix}$ map to λ, then $\lambda_1 = \lambda_2 = \lambda$, hence $\begin{pmatrix} \lambda_1^{-1} & 0 \\ \mathbb{C} & \lambda_1 \end{pmatrix} = \begin{pmatrix} \lambda_2^{-1} & 0 \\ \mathbb{C} & \lambda_2 \end{pmatrix}$.

The map ϕ is also a homomorphism, hence it is an isomorphism. Indeed, using the multiplication law of the quotient group above, we see that

$$\phi(\begin{pmatrix} \lambda^{-1} & 0 \\ \mathbb{C} & \lambda \end{pmatrix} \begin{pmatrix} \tilde{\lambda}^{-1} & 0 \\ \mathbb{C} & \tilde{\lambda} \end{pmatrix}) = \phi(\begin{pmatrix} (\lambda\tilde{\lambda})^{-1} & 0 \\ \mathbb{C} & \lambda\tilde{\lambda} \end{pmatrix}) = \lambda\tilde{\lambda} = \phi(\begin{pmatrix} \lambda^{-1} & 0 \\ \mathbb{C} & \lambda \end{pmatrix})\phi(\begin{pmatrix} \lambda^{-1} & 0 \\ \mathbb{C} & \lambda \end{pmatrix}).$$

Hence, we have shown that $K_2/L_2 \cong \mathbb{C}^*$ (we have found an isomorphism from K_2/L_2 onto $\mathbb{C}^*$).

Let us now consider the homomorphism $\Phi : K_2 \to \mathbb{C}^*$ given by

$$\Phi(\begin{pmatrix} \lambda^{-1} & 0 \\ \mu & \lambda \end{pmatrix}) = \lambda$$

This is onto $\mathbb{C}^*$ (clearly by similar arguments as above), and it is indeed a homomorphism (clearly from the multiplication law above). Its kernel is

$$\begin{aligned} \ker\Phi &= \left\{ \begin{pmatrix} \lambda^{-1} & 0 \\ \mu & \lambda \end{pmatrix}, \lambda \in \mathbb{C}^*,\ \mu \in \mathbb{C} : \Phi(\begin{pmatrix} \lambda^{-1} & 0 \\ \mu & \lambda \end{pmatrix}) = 1 \right\} \\ &= \left\{ \begin{pmatrix} \lambda^{-1} & 0 \\ \mu & \lambda \end{pmatrix} : \lambda = 1, \mu \in \mathbb{C} \right\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in \mathbb{C} \right\} \\ &= L_2 \qquad (10.2) \end{aligned}$$

Hence by the homomorphism theorem we would expect that $K_2/L_2 \cong \mathbb{C}^*$, which is indeed true by the construction above.

11. Automorphisms

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

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

- *Homomorphism: $\phi_a(g_1 g_2) = a g_1 g_2 a^{-1} = a g_1 a^{-1} a g_2 a^{-1} = \phi_a(g_1)\phi_a(g_2)$.*
- *Onto: given $g \in G$, there exists $g' \in G$ such that $\phi_a(g') = g$: indeed, take $g' = a^{-1}ga$.*
- $\mathrm{ker}\phi_a = \{e\}$*: indeed if $\phi_a(g) = e$ then $aga^{-1} = e$ then $g = a^{-1}ea = e$.*

Example 11.2. *Consider $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, with $\mathbb{Z}_2 = \{e, a\}$, $a^2 = e$. Define $\phi : G \to G$ by $\phi((g_1, g_2)) = (g_2, g_1)$. This is an nontrivial (i.e. different from identity map) automorphism. Indeed: 1) it is bijective from G onto G (simple to see), 2) it is nontrivial: $\phi((e,a)) = (a,e) \neq (e,a)$, 3) it is a homomorphism: $\phi(g)\phi(g') = \phi((g_1,g_2))\phi((g_1',g_2')) = (g_2,g_1)(g_2',g_1') = (g_2g_2', g_1g_1') = \phi((g_1g_1', g_2g_2')) = \phi(gg')$. But there is no $g \in \mathbb{Z}_2 \times \mathbb{Z}_2$ such that $\phi = \phi_g$ (that is, such that ϕ is a conjugation by g). Indeed, conjugation by $g = (g_1, g_2)$ gives $\phi_g((e,a)) = (g_1,g_2)(e,a)(g_1^{-1}, g_2^{-1}) = (e, g_2 a g_2^{-1}) \neq (a,e)$ for any g_2.*

Definition 11.2. *For every element $a \in G$, define the map $\phi_a : G \to G$ by $\phi_a(g) = aga^{-1}\ \forall\ g \in G$. An inner automorphism is an automorphism ϕ such that $\phi = \phi_a$ for some $a \in G$. If ϕ is not inner, it is called outer. The set of inner automorphisms of a group G is denoted* $\mathrm{Inn}(G)$*; in symbol, it is simply* $\mathrm{Inn}(G) = \{\phi_a : a \in G\}$.

Definition 11.3. *The set of all automorphisms of a group G is denoted* $\mathrm{Aut}(G)$.

Observe that if G is abelian, then every inner automorphism is the identity map.

Theorem 11.1. *The set of all autmomorphisms* $\mathrm{Aut}(G)$ *is a group under composition. The subset* $\mathrm{Inn}(G)$ *is a normal subgroup.*

Proof. Recall that we have shown in Theorem 3.1 that the set of bijective maps from G to itself is a group, under composition of maps. We need to check that the subset $\mathrm{Aut}(G)$ is a subgroup.

- Closure: Let $\phi_1, \phi_2 \in \mathrm{Aut}(G)$. Then $\phi_1 \circ \phi_2$ is bijective. Also $(\phi_1 \circ \phi_2)(gg') = \phi_1(\phi_2(gg')) = \phi_1(\phi_2(g)\phi_2(g')) = \phi_1(\phi_2(g))\phi_1(\phi_2(g')) = (\phi_1 \circ \phi_2)(g)(\phi_1 \circ \phi_2)(g')$ so the composed map is a homomorphism. Hence it is an automorphism.

- Associativity: derived from the associativity of the group of bijective maps.

- Identity: The identity map is obviously a homomorphism and bijective.

- Inverses: Let $\phi \in \mathrm{Aut}(G)$. For $g_1', g_2' \in G$, let g_1 and g_2 be such that $\phi(g_1) = g_1'$ and $\phi(g_2) = g_2'$ (they exist and are unique by bijectivity). Then, $\phi^{-1}(g_1'g_2') = \phi^{-1}(\phi(g_1)\phi(g_2)) = \phi^{-1}(\phi(g_1g_2)) = g_1g_2 = \phi^{-1}(g_1')\phi^{-1}(g_2')$ so that indeed ϕ^{-1} is homomorphism (hence, again, automorphism).

Second, the subset of inner automorphisms is a subgroup of $\mathrm{Aut}(G)$.

- Closure: $\phi_a \circ \phi_b = \phi_{ab}$: for all $g \in G$, we have $\phi_a(\phi_b(g)) = abgb^{-1}a^{-1} = (ab)g(ab)^{-1}$.

- Associativity: derived from the associativity of the group of bijective maps.

- Identity: ϕ_e is the identity map in $Inn(G)$.

- Inverses: The inverse of ϕ_a is $\phi_{a^{-1}}$.

Now we prove that the subgroup of inner automorphisms is normal. Let ϕ be any automorphism. Then we show that $\phi \circ \phi_a \circ \phi^{-1} = \phi_{\phi(a)}$, so it is indeed an inner automorphism. This is shown as follows: $\phi \circ \phi_a \circ \phi^{-1}(g) = \phi(\phi_a(\phi^{-1}(g))) = \phi(a\phi^{-1}(g)a^{-1}) = \phi(a)g\phi(a^{-1}) = \phi(a)g\phi(a)^{-1} = \phi_{\phi(a)}(g)$ for all $g \in G$. □

Comment(s). *(On notation and automorphisms.)*

1. *Be careful of the meaning of where we put the -1 in the exponent: in $\phi(g^{-1}) = \phi(g)^{-1}$, on the r.h.s. we take the inverse of the element $\phi(g)$. But in $\phi_{a^{-1}}(g) = \phi_a^{-1}(g)$, on the r.h.s. we take the inverse ϕ^{-1} of the map ϕ, and then apply it to g.*

2. *Note the important formulae:*

$$\phi \circ \phi_a \circ \phi^{-1} = \phi_{\phi(a)}, \quad \phi_a \circ \phi_b = \phi_{ab}. \tag{11.1}$$

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

Proof. We only have to realise that the map $\psi : G \to \mathrm{Aut}(G)$ given by $\psi(g) = \phi_g$ is a homomorphism. This holds because $\psi(g_1 g_2) = \phi_{g_1 g_2} = \phi_{g_1} \circ \phi_{g_2} = \psi(g_1)\psi(g_2)$. Hence, we can use the homomorphism theorem, $G/\mathrm{ker}\psi \cong \mathrm{Im}\psi$. Clearly, by definition, $\mathrm{Im}\psi = \mathrm{Inn}(G)$. Let us calculate the kernel. We look for all $g \in G$ such that $\psi(g) = \mathrm{id}$. That is, all g such that $\phi_g(h) = h \; \forall \; h \in G$. This is the set $\{g \in G : ghg^{-1} = h \; \forall \; h \in G\} = \{g \in G : gh = hg \; \forall \; h \in G\} = Z(G)$, so that indeed $\mathrm{ker}\psi = Z(G)$. □

12. Matrix groups

12.1 Basics of matrices

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

Comment(s). *(On matrices.)*

1. *We may multiply matrices in $M_N(\mathbb{R})$ by elements of $\mathbb{R}$ to find a new matrix in $M_N(\mathbb{R})$, for $\lambda \in \mathbb{R}$ and $A \in M_N(\mathbb{R})$ then $\lambda A \in M_N(\mathbb{R})$. We can similarly multiply matrices in $M_N(\mathbb{C})$ by elements of $\mathbb{C}$ to find another element of $M_N(\mathbb{C})$.*

2. *We can combine matrices A and B to find another matrix by*

   (i) *addition: $A + B = C$ where in components $C_{ij} = A_{ij} + B_{ij}$ and*

   (ii) *matrix multiplication: $AB = C$ where, in components, $C_{ij} = \sum_{k=1}^{N} A_{ik}B_{kj}$.*

3. *Under matrix addition the identity element is the matrix of zeroes.*

4. *Under matrix multiplication the identity element is the identity matrix I, where $I_{ij} = \delta_{ij}$.*

5. *Given any matrix A, we may*

   (i) *Take its complex conjugate $\bar{A} : (\bar{A})_{jk} = \overline{A_{jk}}$,*

   (ii) *Take its transpose $A^T : (A^T)_{jk} = A_{kj}$*

   (iii) *Take its adjoint $A^\dagger = \bar{A}^T = \overline{A^T}$.*

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

Definition 12.3. *A matrix A is*

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

Definition 12.4. *The trace of a matrix is* $\mathrm{Tr}(A) = \sum_{j=1}^{N} A_{jj}$.

Exercise 12.1. *Let* A_i *be a set of matrices in* $M_N(\mathbb{R})$*. Prove that*

$$\begin{aligned}\mathrm{Tr}(A_1 A_2 \cdots A_k) &= \mathrm{Tr}(A_k A_1 \cdots A_{k-1}) \\ \mathrm{Tr}(I) &= N.\end{aligned}$$

Definition 12.5. *The Levi-Civita symbol, denoted* $\epsilon_{i_1 i_2 i_3 \cdots i_N}$*, is completely antisymmetric, meaning that its value changes sign when any two neighbouring indices are interchanged, e.g.* $\epsilon_{i_1 i_2 i_3 \cdots i_N} = -\epsilon_{i_2 i_1 i_3 \cdots i_N}$*. It is normalised such that* $\epsilon_{123\cdots N} = 1$.

Comment(s). *(On the Levi-Civita symbol.)*

1. *In two dimensions (N=2), the Levi-Civita symbol has four components:* $\epsilon_{12} = 1$, $\epsilon_{21} = -1$, $\epsilon_{11} = \epsilon_{22} = 0$*. Note that* $\epsilon_{11} = -\epsilon_{11} = 0$ *and similarly for* ϵ_{22}.
2. *In three dimensions (N=3), the Levi-Civita symbol has six non-zero components* $\epsilon_{123} = \epsilon_{231} = \epsilon_{312} = 1$, $\epsilon_{213} = \epsilon_{132} = \epsilon_{321} = -1$.
3. *In three dimensions the Levi-Civita symbol is useful for encoding the vector cross product in components, e.g. if* $\boldsymbol{x} \times \boldsymbol{y} = \boldsymbol{z}$ *then* $z_i = \sum_{j,k=1}^{N} \epsilon_{ijk} x_j y_k$.
4. *The N-dimensional determinant is expressed in terms of the Levi-Civita symbol, as defined below.*

Definition 12.6. *The determinant of a matrix is* $\det(A) = \sum_{j_1=1}^{N} \cdots \sum_{j_N=1}^{N} \epsilon_{j_1 \cdots j_N} A_{1 j_1} \cdots A_{N j_N}$.

Comment(s). *(On the determinant.)*

1. *For* $N = 2$*, we have* $\det(A) = \sum_{j_1=1}^{2} \sum_{j_2=1}^{2} \epsilon_{j_1 j_2} A_{1 j_1} A_{2 j_2} = A_{11} A_{22} - A_{12} A_{21}$.
2. $\det(I) = 1$.
3. $\det(AB) = \det(A)\det(B)$ *(hence, in particular, if* A^{-1} *exists, then* $\det(A^{-1}) = 1/\det(A)$*).*
4. $\det(A) \neq 0$ *if and only if* A *is invertible.*

5. $\det(\bar{A}) = \overline{\det(A)}$.

6. $\det(A^T) = \det(A)$.

7. $\det(\lambda A) = \lambda^N \det(A)$ *(for A a N by N matrix).*

8. *If A is diagonal then* $\det(A) = \prod_{j=1}^{N} A_{jj}$ *(for A a N by N matrix).*

Exercise 12.2. *Prove that* $\det(SAS^{-1}) = \det(A)$.

Exercise 12.3. *Prove that* $\mathrm{Tr}(SAS^{-1}) = \mathrm{Tr}(A)$.

12.2 The Classical Groups as Matrix Groups

These are groups where the group elements are matrices, and the multiplication law is matrix multiplication.

12.2.1 The General Linear Group

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

The group axioms are satisfied:

- Closure: $\det(AB) = \det(A)\det(B) \neq 0$ if $\det(A) \neq 0$ and $\det(B) \neq 0$.
- Associativity: matrix multiplication is associative.
- Identity: $I \in GL(N, \mathbb{C})$ because $\det(I) = 1 \neq 0$.
- Inverses: for every $A \in GL(N, \mathbb{C})$, A^{-1} exists as a matrix because $\det(A) \neq 0$, and $\det(A^{-1}) = 1/\det(A) \neq 0$ so that also $A^{-1} \in GL(N, \mathbb{C})$.

Likewise,

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

and clearly $GL(N, \mathbb{R})$ is a subgroup of $GL(N, \mathbb{C})$.

Theorem 12.1. $\det : GL(N, \mathbb{C}) \to \mathbb{C}^*$ *is a homomorphism onto* $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$*. Also,* $\det : GL(N, \mathbb{R}) \to \mathbb{R}^* := \mathbb{R} \setminus \{0\}$ *is a homomorphism onto* $\mathbb{R}^*$.

Proof. The determinant is onto $\mathbb{C}^*$ as for any $\lambda \in \mathbb{C}^*$ we can always find a matrix A such that $\det(A) = \lambda$: just take $A \in GL(N, \mathbb{C})$ with matrix entries $A_{11} = \lambda$ and $A_{jj} = 1$ for $j > 1$ and $A_{jk} = 0$ for $j \neq k$. It is a homomorphism because $\det(AB) = \det(A)\det(B)$. The proof for $\det : GL(N, \mathbb{R}) \to \mathbb{R}^* := \mathbb{R} \setminus \{0\}$ is identical to the above with the replacement of $\mathbb{C}$ by $\mathbb{R}$. □

12.2.2 The Special Linear Group

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

We will focus on $SL(N,\mathbb{C})$ here but similar statements hold for $SL(N,\mathbb{R})$.

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

Proof. By definition we have $SL(N,\mathbb{C}) = \ker\det$, where by det we mean the map $\det : GL(N,\mathbb{C}) \to \mathbb{C}^*$. Hence, $SL(N,\mathbb{C})$ is a normal subgroup of $GL(N,\mathbb{C})$ (so in particular it is a group.) □

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

Proof. Again consider the homomorphism $\det : GL(N,\mathbb{C}) \to \mathbb{C}^*$, whose kernel is $SL(N,\mathbb{C})$ and which is onto $\mathbb{C}^*$. By the homomorphism theorem the present theorem immediately follows. □

The equivalent statement over the real numbers is $GL(N,\mathbb{R})/SL(N,\mathbb{R}) \cong \mathbb{R}^*$ and is proved in an identical way.

We can make statements about the centres of the general linear and the special linear groups.

Theorem 12.4. *We have $Z(GL(N,\mathbb{C})) \cong \mathbb{C}^*$ and $Z(GL(N,\mathbb{R})) \cong \mathbb{R}^*$.*

Proof. Let $A \in Z(GL(N,\mathbb{C}))$ be such that $AB = BA$ for all $B \in GL(N,\mathbb{C})$. That is,

$$\sum_k A_{ik}B_{kj} = \sum_k B_{ik}A_{kj}.$$

Since this holds for all B, choose B diagonal with diagonal entries all different from each other. There certainly exists such a B in $GL(N,\mathbb{C})$. Then we have

$$A_{ij}B_{jj} = B_{ii}A_{ij} \Rightarrow (B_{ii} - B_{jj})A_{ij} = 0$$

hence $A_{ij} = 0$ for $i \neq j$. Hence, we find that A must be diagonal. Further consider another matrix for B, now take

$$B = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ -1 & 0 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \tag{12.1}$$

This is in $GL(N,\mathbb{C})$ because $\det(B) = 1$. The equation with $i = 1$ and $j = 2$ then gives us $A_{11}B_{12} = B_{12}A_{22}$ hence $A_{11} = A_{22}$. By choosing other matrices B where the 2×2 sub-matrix

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is at different positions along the diagonal, we conclude $A_{jj} = A_{j+1,j+1}$ for all j, so that $A_{jj} = A_{11}$ for all j. Hence $A = \lambda I$ for some $\lambda \in \mathbb{C}$. Since $A \in GL(N, \mathbb{C})$, we must have $\det(A) \neq 0$ hence $\lambda^N \neq 0$ hence $\lambda \neq 0$, i.e. $\lambda \in \mathbb{C}^*$. The group of all diagonal matrices $\{\lambda I : \lambda \in \mathbb{C}^*\}$ is obviously isomorphic to $\mathbb{C}^*$.

A similar proof holds for the real case. □

Theorem 12.5. *$Z(SL(N, \mathbb{C})) \cong \mathbb{Z}_N$. Also $Z(SL(N, \mathbb{R})) \cong \mathbb{Z}_2$ if N is even, and $Z(SL(N, \mathbb{R})) \cong \{1\}$ if N is odd.*

Proof. The first part of the proof for $GL(N, \mathbb{C})$ above goes through in the present case, all the way up to showing that the centres must be matrices proportional to the identity I, of the form $\{\lambda I : \lambda \in \mathbb{C}^*\}$. However for $SL(N, \mathbb{C})$ we require $\det(A) = \lambda^N = 1$, which implies that λ must be an N'th root of unity which are isomorphic to $\mathbb{Z}_N$ (as seen in the examples in chapter 2). Hence we have $Z(SL(N, \mathbb{C})) \cong \mathbb{Z}_N$. For $SL(N, \mathbb{R})$, we find that $A \in Z(SL(N, \mathbb{R}))$ implies that $A = \lambda I$ with $\lambda \in \mathbb{R}^*$, which implies that $\det A = \lambda^N = 1$, hence if N is even we have $\lambda \in \{1, -1\} \cong \mathbb{Z}_2$ and if N is odd we have $\lambda = 1$, i.e.

$$Z(SL(N, \mathbb{R})) \cong \begin{cases} \mathbb{Z}_2 & \text{if N is even} \\ \{1\} & \text{if N is odd.} \end{cases}$$

□

12.2.3 The Unitary Group

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

Observe that the condition $A^\dagger = A^{-1}$ automatically implies that A^{-1} exists, because of course $A^\dagger$ exists for any matrix A; hence it implies that $\det(A) \neq 0$. The condition can also be written $A^\dagger A = AA^\dagger = I$.

- Closure: if $A_1, A_2 \in U(N)$ then $(A_1A_2)^\dagger = A_2^\dagger A_1^\dagger = A_2^{-1}A_1^{-1} = (A_1A_2)^{-1}$ hence $A_1A_2 \in U(N)$.

- Associativity: matrix multiplication is associative.

- Identity: $I^\dagger = I = I^{-1}$ hence $I \in U(N)$.

- Inverses: if $A^\dagger = A^{-1}$ then $(A^{-1})^\dagger = (A^\dagger)^\dagger = A = (A^{-1})^{-1}$, hence that $A^{-1} \in U(N)$.

Hence $U(N)$ is a group.

In the particular case $N = 1$ then

$$U(1) = \{z \in \mathbb{C} : z\bar{z} = 1\}.$$

Writing $z = e^{i\theta}$ we see that the condition $z\bar{z} = 1$ implies $\theta \in \mathbb{R}$; we may restrict to $\theta \in [0, 2\pi)$. Hence $U(1)$ is isomorphic to the group of addition on $\mathbb{R}$ modulo 2π.

Exercise 12.4. *Construct an isomorphism from $U(1)$ to $\mathbb{R}$ equipped with addition modulo 2π.*

Theorem 12.6. *The map* $\det : U(N) \to U(1)$ *is onto and is a group homomorphism.*

Proof. Onto: for $z \in \mathbb{C}$ with $|z| = 1$, we can construct the diagonal matrix $A \in U(N)$ with $A_{11} = z$, $A_{jj} = 1$ for $j > 1$ and all other entries zero. We observe that $A \in U(N)$. Homomorphism: due to the properties of the determinant i.e. $\det(AB) = \det A \det B$. □

12.2.4 The Special Unitary Group

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

As $SU(N) = \ker \det$, where $\det : U(N) \to U(1)$, it is a normal subgroup of $U(N)$. By the homomorphism theorem (with $\phi = \det$ we have:

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

12.2.5 The Orthogonal Group

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

- Closure: if $A, B \in O(N)$ then $(AB)^T = B^T A^T = B^{-1}A^{-1} = (AB)^{-1}$ hence $AB \in O(N)$.
- Associativity: matrix multiplication is associative.
- Identity: $I^T = I = I^{-1}$ hence $I \in O(N)$.
- Inverses: if $A^T = A^{-1}$ then $(A^{-1})^T = (A^T)^T = A$, so $A^{-1} \in O(N)$.

This is the group of orthogonal matrices. Observe that $O(N)$ consists of real matrices and is a subgroup of $U(N)$. Also, observe that if $A \in O(N)$ then $A^T A = I$ so that $\det(A)^2 = 1$. Hence

$\det(A) = \pm 1 \cong \mathbb{Z}_2$. In fact, there are $A \in O(N)$ with $\det(A) = 1$ (take $A = I$) and with $\det(A) = -1$ (take

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

which satisfies $A^T A = I$). Hence, $\det : O(N) \to \mathbb{Z}_2$ is a homomorphism onto $\mathbb{Z}_2$.

12.2.6 The Special Orthogonal Group

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

As before $SO(N) = \ker \det$ for $\det : O(N) \to \mathbb{Z}_2$, hence $SO(N)$ is a normal subgroup of $O(N)$. Hence by the homomorphism theorem we have

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

Theorem 12.7. *If N is odd, $O(N) \cong \mathbb{Z}_2 \times SO(N)$.*

Proof. Let us construct an isomorphism ϕ that does the job:

$$\phi : O(N) \to \mathbb{Z}_2 \times SO(N) \text{ given by } \phi(A) = \left(\det(A), \frac{A}{\det(A)}\right)$$

for $A \in O(N)$. We have to show that this is well-defined (i.e. that ϕ maps into the specified space - we must do this because it is not immediately obvious a priori), and then that it is indeed an isomorphism.

First: that it maps into $\mathbb{Z}_2 \times SO(N)$ is shown as follows. 1) Clearly $\det(A) \in \mathbb{Z}_2$ by the discussion above. 2) Also $(A/\det(A))^T = A^T/\det(A) = A^{-1}/\det(A)$ and $(A/\det(A))^{-1} = A^{-1}\det(A) = A^{-1}/\det(A)$ where in the last step we used $\det(A)^2 = 1$. Hence these are equal, so that $A/\det(A) \in O(N)$. 3) Further, $\det(A/\det(A)) = \det(A)/\det(A)^N = \det(A)^{1-N} = (\pm 1)^{1-N}$. If N is odd, then $N - 1$ is even, so $(\pm 1)^{1-N} = 1$. Hence indeed $\det(A/\det(A)) = 1$ so $A/\det(A) \in SO(N)$.

Second: that it is a homomorphism:

$$\begin{aligned}\phi(AB) &= \left(\det(AB), \frac{AB}{\det(AB)}\right)\\ &= \left(\det(A)\det(B), \frac{A}{\det(A)}\frac{B}{\det(B)}\right)\\ &= \left(\det(A), \frac{A}{\det(A)}\right)\left(\det(B), \frac{B}{\det(B)}\right)\\ &= \phi(A)\phi(B)\end{aligned}$$

Third: that it is bijective. Injectivity: if $\phi(A_1) = \phi(A_2)$ then $\det(A_1) = \det(A_2)$ and $A_1/\det(A_1) = A_2/\det(A_2)$, hence combining these, $A_1 = A_2$, so indeed it is injective. Surjectivity: take $a \in \mathbb{Z}_2 \cong \{-1, 1\}$ and $B \in SO(N)$. We can always find a matrix $A \in O(N)$ such that $\phi(A) = (a, B)$. Indeed, just take $A = aB$. This is indeed in $O(N)$: we have $A^T = (aB)^T = aB^T$ and $A^{-1} = (aB)^{-1} = a^{-1}B^{-1} = aB^T$, so both are equal (we used $a^{-1} = a$ for $a \in \mathbb{Z}_2$ and $B^{-1} = B^T$ 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 $B \in SO(N)$). Hence, $\phi(A) = (a, A/a) = (a, B)$, which shows surjectivity. □

The proof above only works for odd N, for even N we will need to develop the semi-direct product, which we will do in the following chapter of this course.

Each matrix group has infinite order (due to the matrix entries being real or complex numbers), so instead of order it is useful to consider the number of real parameters needed to specify a general matrix in each matrix group. This is the real dimension of the matrix group. The (real) dimensions for some of the matrix groups we have met are

- $GL(N, \mathbb{R})$: N^2 dimensions.
- $SL(N, \mathbb{R})$: $N^2 - 1$ dimensions due to the one condition $\det(A) = 1$.
- $SO(N)$: $N(N-1)/2$ dimensions. Indeed: there are $N \times N$ real matrices so there are N^2 parameters. There is the condition $A^TA = I$. This is a condition on the matrix A^TA, which contains N^2 elements. But this matrix is symmetric no matter what A is, because $(A^TA)^T = A^TA$. Hence, the constraint $A^TA = I$ in fact has $1 + 2 + ... + N$ constraints only (looking at the top row with N elements, then the second row with $N - 1$ elements, etc.). That is, $N(N + 1)/2$ constraints. These are independent constraints. Hence, the dimension is $N^2 - N(N + 1)/2 = N(N - 1)/2$.

The classical matrix groups are examples of Lie groups which are manifolds[1] equipped with a group structure. Lie groups are characterised by having a continuum of elements (rather than the discrete elements we see in the case of finite groups) which can be labelled by a continuous parameter. It is interesting to investigate the structure of the underlying shape (manifold) to which each point in the space is associated an element of the matrix group. One of the simplest examples to study is $SO(2)$.

[1] For the purposes of this course, a manifold is a geometric object which locally is equivalent to Euclidean space (and satisfies several technical properties which we do not state here). S^2 is an example of a manifold: a local coordinate chart is like the coordinates on a page in an atlas and there exist smooth maps between pages in the atlas which tell the reader how to reconnect the pages of the atlas to cover S^2. The manifold is the fundamental object in the study of differential geometry.

13. The Structure of Some Matrix Groups

13.1 $SO(2)$

Let us explicitly construct the matrix group $SO(2)$:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad A^T A = I, \quad \det(A) = 1.$$

Now

$$A^T A = I \Rightarrow a^2 + c^2 = 1,\ b^2 + d^2 = 1,\ ab + cd = 0$$

while

$$AA^T = I \Rightarrow a^2 + b^2 = 1,\ c^2 + d^2 = 1,\ ac + bd = 0.$$

The conditions imply, without loss of generality, that

$$a = \pm\cos\theta = d, \quad \text{and} \quad c = \pm\sin\theta = b.$$

The remaining conditions to be satisfied are $ac = -bd$ and $ab = -cd$. Together with the condition that $\det A = 1$, i.e. $ad - bc = 1$ leads to the consistent choice of signs given by $a = d = \cos\theta$ and $c = -b = \sin\theta$, giving

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

Note that is of real dimension 1 as there is one real parameter θ needed to specify any matrix $A(\theta) \in SO(2)$.

Explicit multiplication of matrices gives

$$A(\theta)A(\theta') = A(\theta + \theta'), \quad A(\theta)^{-1} = A(-\theta)$$

In particular, $SO(2)$ is abelian.

The group $SO(2)$ is isomorphic with the circle S^1, as it is parameterised by $\theta \in S^1$. Every point on S^1 corresponds to a unique group element $\theta \mapsto A(\theta)$, the group $SO(2)$ is covered in this way. N.B. Geometrically, the structure of $SO(2)$ is indeed S^1 rather than the interval $[0, 2\pi)$ because of periodicity, i.e. continuity from the endpoint 2π back to the starting point 0.

The matrices of $SO(2)$ are the rotation matrices acting on the plane $\mathbb{R}^2$ and rotating it about the origin as

$$v' = Av, \quad A \in SO(2),\ v = \begin{pmatrix} x \\ y \end{pmatrix},\ (x, y) \in \mathbb{R}^2.$$

This gives

$$x' = x\cos\theta - y\sin\theta, \quad y' = x\sin\theta + y\cos\theta$$

We can also represent rotations of the plane about the origin by multiplications of $e^{i\theta}$ on the complex plane. Hence $\phi(A(\theta)) = e^{i\theta}$ gives an isomorphism $SO(2) \cong U(1)$.

13.2 $SU(2)$ and the Pauli Matrices

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

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

we have from $A^\dagger = A^{-1}$ i.e.

$$\begin{pmatrix} \alpha^* & \gamma^* \\ \beta^* & \delta^* \end{pmatrix} = \frac{1}{\alpha\delta - \beta\gamma} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}.$$

Now $\det(A) = \alpha\delta - \beta\gamma = 1$ hence we find that $\alpha^* = \delta$ and $\gamma^* = -\beta$. Therefore any matrix $A \in SU(2)$ takes the form

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

Writing the complex numbers in terms of their real components with $\alpha = a + ib_z$ and

$\beta = b_y + ib_x$ we have

$$\begin{aligned} A &= \begin{pmatrix} a+ib_z & b_y+ib_x \\ -b_y+ib_x & a-ib_z \end{pmatrix} \\ &= a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + ib_z\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + ib_y\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + ib_x\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &\equiv aI + ib_x\sigma_x + ib_y\sigma_y + ib_z\sigma_z \\ &= aI + i\boldsymbol{b}\cdot\boldsymbol{\sigma} \qquad \text{with} \quad a^2+b_x^2+b_y^2+b_z^2 = 1. \end{aligned}$$

where we understand $\boldsymbol{\sigma}$ as a vector of matrices, with components

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

so that $\boldsymbol{b}\cdot\boldsymbol{\sigma} = b_x\sigma_x + b_y\sigma_y + b_z\sigma_z$. The matrices σ_x, σ_y and σ_z are called the Pauli matrices.

Comment(s). *On the Pauli matrices...*

1. $\mathrm{Tr}(\sigma_i) = 0$.

2. $\sigma_i = \sigma_i^\dagger$.

3. *The Pauli matrices form a basis for the traceless* 2×2*, unitary* ($MM^\dagger = I$)*, Hermitian* ($M = M^\dagger$) *matrices. Note that a matrix M being both unitary and Hermitian implies that* $M = M^{-1}$.

4. $\sigma_i^2 = I$.

5. $\sigma_i\sigma_j = -\sigma_j\sigma_i$ *for* $i \neq j$.

6. $\sigma_x\sigma_y = i\sigma_z$, $\sigma_y\sigma_z = i\sigma_x$ *and* $\sigma_z\sigma_x = i\sigma_y$. *By writing* $\sigma_1 \equiv \sigma_x$, $\sigma_2 \equiv \sigma_y$ *and* $\sigma_3 \equiv \sigma_z$ *we can write these relations in a compact form as* $\sigma_i\sigma_j = i\sum_k \epsilon_{ijk}\sigma_k$ *where* ϵ_{ijk} *is the Levi-Civita symbol, which is completely antisymmetric in its indices and normalised with* $\epsilon_{123} = 1$.

7. $[\sigma_i, \sigma_j] = \sigma_i\sigma_j - \sigma_j\sigma_i = 2\sigma_i\sigma_j = 2i\sum_k \epsilon_{ijk}\sigma_k$ *where* $\sigma_1 \equiv \sigma_x$, $\sigma_2 \equiv \sigma_y$ *and* $\sigma_3 \equiv \sigma_z$.

These properties point to a nice analogy with the complex numbers. Note that as $(i\sigma_i)^2 = -I$ then $i\sigma_x$, $i\sigma_y$ and $i\sigma_z$ each act like a matrix version of an imaginary number. Unlike the complex numbers where there is only one basis imaginary number $i = \sqrt{-1}$, here we have three distinct matrix imaginary numbers. In fact these matrices give a natural extension of the complex numbers to the quaternions.

Definition 13.1. *The division algebra* $\mathbb{H}$ *of quaternions is the non-commutative algebra of all real linear combinations* $z = a + b_z\hat{\imath} + b_y\hat{\jmath} + b_x\hat{\mathrm{k}}$ *(*$a, b_x, b_y, b_z \in \mathbb{R}$*), with the relations* $\hat{\imath}^2 = \hat{\jmath}^2 = \hat{\mathrm{k}}^2 = -1$ *and* $\hat{\imath}\hat{\jmath} = -\hat{\jmath}\hat{\imath} = \hat{\mathrm{k}}$ *and cyclic permutations.*

To compare with our matrix representation of the imaginary quaternions we write $\hat{\imath} = i\sigma_z$, $\hat{\jmath} = i\sigma_y$, $\hat{\mathrm{k}} = i\sigma_x$. We pick this choice of association so that $\hat{\imath}\hat{\jmath}\hat{\mathrm{k}} = (i\sigma_z)(i\sigma_y)(i\sigma_x) = (i\sigma_z)(i\sigma_z) = -I^2$, an alternative defining relation for the quaternions, together with $\hat{\imath}^2 = \hat{\jmath}^2 = \hat{\mathrm{k}}^2 = -I$. One can show that this algebra is associative.

One defines the quaternion conjugate by

$$\bar{z} = a - b_z\hat{\imath} - b_y\hat{\jmath} - b_x\hat{\mathrm{k}}$$

and from the point of view of the two by two matrices this is $\bar{z} = z^\dagger$ and, further, we have $z\bar{z} = \bar{z}z = a^2 + |\boldsymbol{b}|^2 \geq 0$, with equality iff $z = 0$. Hence we can define $|z| = \sqrt{z\bar{z}}$ and also $z^{-1} = \bar{z}/|z|^2$, as for the complex numbers. An important identity is $|z_1 z_2| = |z_1|\,|z_2|$ for any $z_1, z_2 \in \mathbb{H}$, which follows from $|z_1 z_2|^2 = z_1 z_2 \bar{z}_2 \bar{z}_1 = z_2 \bar{z}_2 z_1 \bar{z}_1$ where we used the fact that $z_2\bar{z}_2 \in \mathbb{R} \subset \mathbb{H}$ hence commutes with everything. Any quaternion z has a unique inverse, except for 0. This is what makes the quaternions a division algebra: we have addition and multiplication (of $\mathbb{H}\backslash\{0\}$), with unique inverses and identity elements (0 is the additive identity and 1 is the multiplicative identity). Note that there are no other associative division algebras apart from $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$. There is another division algebra, the octonions, but it is not associative (the octonians have 7 imaginary numbers).

In terms of quaternions, the above description of $SU(2)$ is:

$$SU(2) = \{z \in \mathbb{H} : |z| = 1\}.$$

Note the similarity with

$$U(1) = \{z \in \mathbb{C} : |z| = 1\}$$

In both cases we have a group partly because in both cases $|z_1 z_2| = |z_1|\,|z_2|$, so the condition $|z| = 1$ is preserved under multiplication.

Geometrically the condition $|z| = 1$ for quaternions is the condition for a 3-sphere in $\mathbb{R}^4$. This is the manifold of $SU(2)$ i.e.

$$\det \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} = |\alpha|^2 + |\beta|^2 = a^2 + b_x^2 + b_y^2 + b_z^2 = 1$$

which is the condition for a point (a, b_x, b_y, b_z) in $\mathbb{R}^4$ to lie on a three sphere S^3.

13.3 Invariant Inner Products: $O(N)$ and $U(N)$

In this section the groups $O(N)$ and $U(N)$ will be understood as symmetry groups of an inner product on a complex vector space.

13.3.1 The Inner Product

Let V be a finite-dimensional vector space over $\mathbb{C}$. A map $V \times V \to \mathbb{C}$, $\boldsymbol{x}, \boldsymbol{y} \mapsto (\boldsymbol{x}, \boldsymbol{y})$ is an inner product if it has the properties:

$$(\boldsymbol{x}, \boldsymbol{y})^* = (\boldsymbol{y}, \boldsymbol{x}), \quad (\boldsymbol{x}, a\boldsymbol{y} + b\boldsymbol{z}) = a(\boldsymbol{x}, \boldsymbol{y}) + b(\boldsymbol{x}, \boldsymbol{z}), \quad (\boldsymbol{x}, \boldsymbol{x}) \geq 0, \quad (\boldsymbol{x}, \boldsymbol{x}) = 0 \Rightarrow \boldsymbol{x} = 0$$

($z^* = \bar{z}$ is the complex conjugate). The existence of the inner product on V is sufficient for V to be a Hilbert space. Note that the first and second property imply

$$(a\boldsymbol{y} + b\boldsymbol{z}, \boldsymbol{x}) = a^*(\boldsymbol{y}, \boldsymbol{x}) + b^*(\boldsymbol{z}, \boldsymbol{x}).$$

This along with the second property is called sesquilinearity (a generalisation of bilinearity[1]). The restriction over the real-vector space (real restriction: $\mathbb{C}^N$ becomes $\mathbb{R}^N$; “same” basis, but only consider real coefficients) then gives

$$(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{y}, \boldsymbol{x}), \quad (a\boldsymbol{y} + b\boldsymbol{z}, \boldsymbol{x}) = a(\boldsymbol{y}, \boldsymbol{x}) + b(\boldsymbol{z}, \boldsymbol{x}).$$

This restriction is bilinear and symmetric. The only example we will use is:

$$(\boldsymbol{x}, \boldsymbol{y}) = \sum_i x_i^* y_i.$$

In particular, using matrix and column vector notation, this is

$$(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{x}^\dagger \boldsymbol{y}.$$

This implies that if A is a linear operator, then

$$(\boldsymbol{x}, A\boldsymbol{y}) = (A^\dagger \boldsymbol{x}, \boldsymbol{y}).$$

The norm of a vector is defined by

$$||\boldsymbol{x}|| = \sqrt{(\boldsymbol{x}, \boldsymbol{x})}$$

(positive square-root). Note that on a Euclidean vector space it is commonplace to use $|\boldsymbol{x}|$ to denote the length of a vector (the absolute value norm), while on a general vector space equipped with an inner product the notation $||\boldsymbol{x}||$ is used, consequently it is not uncommon to see only $|\boldsymbol{x}|$ used when there is an underlying Euclidean inner product in a vector space.

[1] If we were to restrict V to be a real vector space so that $a, b \in \mathbb{R}$ then as $a^* = a$, $b^* = b$ we would have a bilinear symmetric inner product from the conditions listed above.

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

Theorem 13.1. *A real, linear transformation A of $\mathbb{R}^N$ is such that $||A\boldsymbol{x}|| = ||\boldsymbol{x}||$ for all $\boldsymbol{x} \in \mathbb{R}^N$ iff $A \in O(N)$.*

Proof. First direction: If $A \in O(N)$, then $A^T = A^{-1}$ so that

$$\begin{aligned} ||A\boldsymbol{x}||^2 &= (A\boldsymbol{x}, A\boldsymbol{x}) \\ &= (A\boldsymbol{x})^T A\boldsymbol{x} \\ &= \boldsymbol{x}^T A^T A\boldsymbol{x} \\ &= \boldsymbol{x}^T \boldsymbol{x} \\ &= ||\boldsymbol{x}||^2 \end{aligned} \tag{13.1}$$

where in the second step we use reality, so that $^\dagger =^T$.

Second direction: If $||A\boldsymbol{x}|| = ||\boldsymbol{x}||$, then

$$\begin{aligned} ||A\boldsymbol{x}||^2 &= \sum_i (\sum_j A_{ij}x_j)^\dagger)(\sum_k A_{ik}x_k)) \\ &= \sum_{i,j,k} x_j^T (A_{ij})^T A_{ik} x_k \\ &= ||\boldsymbol{x}||^2 \end{aligned}$$

in the last line we have used the assumption that $||A\boldsymbol{x}|| = ||\boldsymbol{x}||$. In component notation

$$||\boldsymbol{x}||^2 = \sum_j x_j^T x_j = \sum_{j,k} x_j^T \delta_{jk} x_k.$$

So we have

$$\sum_{i,j,k} x_j^T (A_{ij})^T A_{ik} x_k = \sum_{j,k} x_j^T \delta_{jk} x_k$$

and for this to hold for all $\boldsymbol{x} \in \mathbb{R}^N$ we must have

$$\sum_i (A_{ij})^T A_{ik} = \delta_{jk}$$

which in matrix notation is

$$A^T A = I$$

which implies that $A \in O(N)$. □

Theorem 13.2. *If $\boldsymbol{x} \in \mathbb{C}^N$ is an eigenvector of $A \in O(N)$ with eigenvalue λ, then $|\lambda| = 1$.*

Proof. $A\boldsymbol{x} = \lambda\boldsymbol{x}$ with $\boldsymbol{x} \neq 0$, hence $(A\boldsymbol{x}, A\boldsymbol{x}) = (\lambda\boldsymbol{x}, \lambda\boldsymbol{x})$ hence $(\boldsymbol{x}, \boldsymbol{x}) = |\lambda|^2(\boldsymbol{x}, \boldsymbol{x})$ hence $|\lambda|^2 = 1$ since $\boldsymbol{x} \neq 0$. □

If a complex, linear transformation preserves the length of a vector in $\mathbb{C}^N$ then the transformation is an element of the unitary group $U(N)$:

Theorem 13.3. *A complex, linear transformation A on $\mathbb{C}^N$ preserves the norm, $||A\boldsymbol{x}|| = ||\boldsymbol{x}||$ for all $\boldsymbol{x} \in \mathbb{C}^N$, iff $A \in U(N)$.*

Proof. We must prove this in both directions.

1. If $A \in U(N)$ then $||A\boldsymbol{x}||^2 = (A\boldsymbol{x}, A\boldsymbol{x}) = \boldsymbol{x}^\dagger A^\dagger A\boldsymbol{x} = \boldsymbol{x}^\dagger\boldsymbol{x} = (\boldsymbol{x}, \boldsymbol{x}) = ||\boldsymbol{x}||^2$ hence $||A\boldsymbol{x}|| = ||\boldsymbol{x}||$.

2. Let A denote any complex, linear transformation which preserves the norm. Then $||A\boldsymbol{x}|| = ||\boldsymbol{x}||$ implies that $(A\boldsymbol{x}, A\boldsymbol{x}) = (A^\dagger A\boldsymbol{x}, \boldsymbol{x}) = (\boldsymbol{x}, \boldsymbol{x})$ which implies that $A^\dagger A = I$ hence $A \in U(N)$.

□

13.4 SO(3)

Theorem 13.4. *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 $P(\lambda) = \det(A - \lambda I)$. We know that $P(0) = 1$ because $A \in SO(3)$. Also, $P(\lambda) = -\lambda^3 + \ldots + 1$ because the only order-3 term in the determinant is from the $-\lambda I$ part. Hence, $P(\lambda) = -(\lambda - \lambda_1)(\lambda - \lambda_2)(\lambda - \lambda_3)$ for some $\lambda_{1,2,3}$ with $\lambda_1\lambda_2\lambda_3 = 1$. Our aim is to show that at least one of these eigenvalues must equal one. There are two possibilities:

1. If one of these eigenvalues, say λ_1, is complex then as Theorem 13.2 holds ($A \in SO(N) \subset O(N)$ then $|\lambda_1| = 1$ so $\lambda_1 = e^{i\alpha}$ for $\alpha \in (0, 2\pi) - \{\pi\}$ (this set excludes $\lambda_1 = -1$ as λ_1 is not real by assumption). If $\boldsymbol{x}$ is the associated eigenvector, it cannot be real and $A\boldsymbol{x} = e^{i\alpha}\boldsymbol{x}$ hence $A^*\boldsymbol{x}^* = e^{-i\alpha}\boldsymbol{x}^*$ so that $\boldsymbol{x}^*$ is a new eigenvector with a different eigenvalue, say $\lambda_2 = e^{-i\alpha}$. But since $\lambda_1\lambda_2\lambda_3 = 1$, it must be that $\lambda_3 = 1$.

2. If all λ_i are real, then $\lambda_i = \pm 1$. Since $\lambda_1\lambda_2\lambda_3 = 1$, the option where all three are -1 is ruled out, hence at least one is 1.

Finally we show that if $\boldsymbol{x}$ is the eigenvector with eigenvalue one (which may not be a real eigenvector) then there exists a real eigenvector $\boldsymbol{n}$ with eigenvalue one. Given $A\boldsymbol{x} = \boldsymbol{x}$ with

$\boldsymbol{x} \in \mathbb{C}^3$ such that $\boldsymbol{x} \neq \boldsymbol{x}^*$ then $A\boldsymbol{x}^* = \boldsymbol{x}^*$ and so $\boldsymbol{x}^*$ is another eigenvector with eigenvalue one. We have $\lambda_1 = 1$, $\lambda_2 = 1$ then as $\lambda_1\lambda_2\lambda_3 = 1$ so $\lambda_3 = 1$ too). Hence all three eigenvectors have eigenvalue one. Now $A(\boldsymbol{x} + \boldsymbol{x}^*) = \boldsymbol{x} + \boldsymbol{x}^*$ so $\boldsymbol{n} = \boldsymbol{x} + \boldsymbol{x}^*$ is a real eigenvector with eigenvalue one. □

We may normalise to $||\boldsymbol{n}|| = 1$. Suppose $\boldsymbol{n} = \hat{\boldsymbol{e}}_x$ (unit vector in x direction). Then $A\hat{\boldsymbol{e}}_x = \hat{\boldsymbol{e}}_x$ implies

$$A = \begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$$

Further, $A^T A = I$ implies

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$$

The 2 by 2 matrix in the bottom-right, which we denote a, has the property

$$a^T a = I, \quad \det(a) = 1$$

hence it is an $SO(2)$ matrix. Hence,

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}. \tag{13.2}$$

That is, A is a rotation by θ around the x axis. In general, A will be a rotation about the axis spanned by $\boldsymbol{n}$, i.e. the axis $\{c\boldsymbol{n} : c \in \mathbb{R}\}$, if $A\boldsymbol{n} = \boldsymbol{n}$. Hence, an $SO(3)$ matrix is always a rotation with respect to a certain axis. But also, any rotation is in $SO(3)$. Clearly, if A is a rotation, then $(A\boldsymbol{x}, A\boldsymbol{x}) = (\boldsymbol{x}, \boldsymbol{x})$ for any $\boldsymbol{x} \in \mathbb{R}^3$, so $A \in O(3)$. Also, if A is a rotation with respect to an axis spanned by $\boldsymbol{n}$, then $A\boldsymbol{n} = \boldsymbol{n}$, and further in a right-handed orthonormal basis that where $\boldsymbol{n} = \hat{\boldsymbol{e}}_x$, a rotation A always has the form shown in equation (13.2). Hence $A \in SO(3)$. That is:

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

Geometrically, given a vector $\boldsymbol{x}$ in $\mathbb{R}^3$ we may use it to define a right-handed rotation about the axis spanned by $\boldsymbol{x}$. If we suppose that the length of the vector is used to denote the angle of rotation about the axis then we can represent all rotations in $\mathbb{R}^3$ by the set of vectors which form the ball of radius 2π. That is, each point in the ball represents a vector from the origin to that point - it has length $|\boldsymbol{x}| \in [0, 2\pi]$ and defines an axis parallel to $\boldsymbol{x}$ about which the rotation occurs. However because both $\boldsymbol{x}$ and $-\boldsymbol{x}$ span the same axis and have the same length they represent similar rotations: the only difference is that one rotates clockwise about the axis and the other counter-clockwise - due to the $\boldsymbol{x}$ and $-\boldsymbol{x}$ pointing in opposite directions (and applying the right-hand-rule to determine the direction of rotation). With some thought you can see that the rotation represented by the vector $\boldsymbol{x}$ of length θ is equivalent to the vector pointing in the opposite direction and with length $2\pi - \theta$ (think of rotations in the plane to convince yourself of this). Hence we would be overcounting the number of rotations. To remove the repeated rotations we reduce the radius of the ball from 2π to π and note that points which lie on the surface of the ball and lie on same axis through the origin correspond to the same rotation. Hence these points must be identified in this geometric picture of $SO(3)$. To summarise, the manifold of $SO(3)$ is the ball of radius π in $\mathbb{R}^3$ with diametrically opposed points being identified.

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

Recall that if $A \in SU(2)$ then

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

for $\alpha, \beta \in \mathbb{C}$. Writing $\alpha = u + iv$ and $\beta = x + iy$ for $u, v, x, y \in \mathbb{R}$ gives $1 = |\alpha|^2 + |\beta|^2 = u^2 + v^2 + x^2 + y^2$. This is the equation for $S^3 \in \mathbb{R}^4$ and each point $(u, v, x, y) \in S^3$ encodes a matrix $A \in SU(2)$. To picture S^3, imagine taking cross-sectional slices of $S^3 \in \mathbb{R}^4$ (each cross-section of $\mathbb{R}^4$ is $\mathbb{R}^3$ which is three-dimensional, so the cross-sectional slices of S^3 will be two-dimensional or sometimes one-dimensional surfaces in $\mathbb{R}^3$). A slice at the pole gives only a point, to see this consider the pole with coordinates $u = 1$ then we have

$$v^2 + x^2 + y^2 = 0 \implies v = x = y = 0$$

hence a single point with coordinates $(u, v, x, y) = (1, 0, 0, 0)$. Now move along the sphere decreasing u from $u = 1$ towards $u = 0$: when $0 < u < 1$ we have

$$v^2 + x^2 + y^2 = 1 - u^2 > 0$$

for fixed $u = u_0$ with $0 < u_0 < 1$ we find a set of v, x and y coordinates which satisfy

$$v^2 + x^2 + y^2 = 1 - {u_0}^2$$

i.e. (v, x, y) are points on a sphere, S^2, of radius $\sqrt{1 - {u_0}^2}$ in $\mathbb{R}^3$. For each fixed value of the coordinate $0 < u < 1$ we find a sphere S^2 of radius $\sqrt{1 - u^2}$ as u varies from $u = 1$ towards

$u = 0$. For $-1 < u < 0$ we find a similar set of S^2's. If we nest all these spheres together (corresponding to $-1 < u < 0$ and $0 < u < 1$) we can construct two copies of the open ball in $\mathbb{R}^3$. From the cross-sections when $u = \pm 1$ we find two points, corresponding to spheres of radius zero which form the central point of each open ball. We have only one cross-section to consider when $u = 0$ when we have

$$v^2 + x^2 + y^2 = 1$$

which is a sphere of unit radius. Now we may split this sphere into two hemispheres and place one on each of the two open balls, to give two copies of a structure we have met earlier in these lectures. Recall that $SO(3)$ geometrically has the structure of a ball of radius π with diametrically-opposed points on the surface being identified. From the cross-sections of $SU(2)$ we constructed two copies of this structure underlying $SO(3)$. We might reasonably wonder if $SU(2)$ is the double-cover of $SO(3)$.

Theorem 13.5. *$SU(2)/\mathbb{Z}_2 \cong SO(3)$.*

Proof. This proof is not complete, but the main ingredients are there: it is a sketch of the full proof. The idea of the proof is to use the homomorphism theorem, with a homomorphism $\varphi : SU(2) \to SO(3)$ that is onto, such that $\ker \varphi \cong \mathbb{Z}_2$.

Proposition 13.5.1. *There exists a linear bijective map $\Theta : \Sigma \to \mathbb{R}^3$ where Σ is the real, linear space of self-adjoint, traceless two-by-two matrices.*

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

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

it is evidently bijective but it is also linear as

$$\begin{aligned}\Theta(cA) &= \Theta(c\boldsymbol{b} \cdot \boldsymbol{\sigma}) = c\boldsymbol{b} = c\Theta(\boldsymbol{b} \cdot \boldsymbol{\sigma}) = c\Theta(A)\\ \Theta(A + A') &= \Theta(\boldsymbol{b} \cdot \boldsymbol{\sigma} + \boldsymbol{b}' \cdot \boldsymbol{\sigma}) = \Theta((\boldsymbol{b} + \boldsymbol{b}') \cdot \boldsymbol{\sigma}) = \boldsymbol{b} + \boldsymbol{b}' = \Theta(A) + \Theta(A').\end{aligned}$$

Hence Θ is a linear map. This completes the proof of the proposition. □

Armed with the proposition, we return to the outline of the proof of theorem 13.5.

Given any $U \in SU(2)$, we can form a linear bijective map $\Phi_U : \Sigma \to \Sigma$ as follows:

$$\Phi_U(A) = UAU^\dagger.$$

This maps into Σ because if $A \in \Sigma$, then 1) $\mathrm{Tr}(\Phi_U(A)) = \mathrm{Tr}(UAU^\dagger) = \mathrm{Tr}(U^\dagger UA) = \mathrm{Tr}(A) = 0$, and 2) $(UAU^\dagger)^\dagger = UA^\dagger U^\dagger = UAU^\dagger$. Hence, $\Phi_U(A) \in \Sigma$. Moreover, it is bijective because 1) injectivity: if $UAU^\dagger = UA'U^\dagger$ then $U^\dagger UAU^\dagger U = U^\dagger UA'U^\dagger U$ hence $A = A'$, and 2) surjectivity: for any $B \in \Sigma$, we have that $U^\dagger BU \in \Sigma$ (by the same arguments as above) and we have $\Phi_U(U^\dagger BU) = UU^\dagger BU^\dagger U = B$ so we have found a $A = U^\dagger BU \in \Sigma$ that maps to B. Finally it is evidently linear.

Together the maps $\Theta : \Sigma \to \mathbb{R}^3$ and $\Phi_U : \Sigma \to \Sigma$ together induce a map on $\mathbb{R}^3$. We define $R_U : \mathbb{R}^3 \to \mathbb{R}^3$ by

$$R_U = \Theta \circ \Phi_U \circ \Theta^{-1}$$

for any $U \in SU(2)$. By the properties of Φ_U and of Θ derived above we have that R_U is linear and bijective.

We now want to show that $R_U \in SO(3)$.

1. From the properties of Pauli matrices, we know that $\det(\boldsymbol{b} \cdot \boldsymbol{\sigma}) = -||\boldsymbol{b}||^2$. Hence, we have for any $A \in \Sigma$ that $\det(A) = -||\Theta(A)||^2$, or in other words $\det(\Theta^{-1}(\boldsymbol{b})) = -||\boldsymbol{b}||^2$. Hence,

$$\begin{aligned} ||R_U(\boldsymbol{b})||^2 &= ||\Theta(\Phi_U(\Theta^{-1}(\boldsymbol{b})))||^2 \\ &= -\det(\Phi_U(\Theta^{-1}(\boldsymbol{b}))) \\ &= -\det(U\Theta^{-1}(\boldsymbol{b})U^\dagger) \\ &= -\det(\Theta^{-1}(\boldsymbol{b})) \\ &= ||\boldsymbol{b}||^2. \end{aligned}$$

   That is, R_U is a real-linear map on $\mathbb{R}^3$ that preserves lengths of vectors. By the previous theorems, it must be that $R_U \in O(3)$.

2. Further, the map $g : SU(2) \to \mathbb{R}$ given by $g(U) = \det(R_U)$ (where we see the linear map R_U as a 3 by 3 real orthogonal matrix). This is continuous as a function of the matrix elements of U. Indeed, we can calculate any matrix element of R_U by choosing two basis vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{R}^3$ and by computing $\boldsymbol{x} \cdot R_U(\boldsymbol{y})$. This is $\boldsymbol{x} \cdot \Theta(U\Theta^{-1}(\boldsymbol{y})U^\dagger)$. The operation $U \mapsto U^\dagger$ and the operations of matrix multiplications are continuous in the matrix elements, hence the map $U \mapsto U\Theta^{-1}(\boldsymbol{y})U^\dagger$ is, for any matrix element of the resulting 2 by 2 matrix, continuous in the matrix elements of U. Since Θ is linear, it is also continuous, and finally the dot-product operation is continuous. Hence, all matrix

elements of R_U are continuous functions of the matrix elements of U, so that $\det(R_U)$ is also a continuous function of the matrix elements of U. Moreover, we know that with $U = I$, we find $R_U = I$ (the former: identity 2 by 2 matrix, the latter: identity 3 by 3 matrix). Hence, $g(I) = 1$. But since $g(U) \in \{1, -1\}$ (because the determinant of an $O(3)$ matrix is ± 1), it must be that $g(U) = 1$ for all $U \in SU(2)$ that can be reached by a continuous path from I (indeed, if $\gamma : [0, 1] \to SU(2)$ is such a continuous path, $\gamma(0) = I$ and $\gamma(1) = U$ and $\gamma(t)$ a continuous function of t, then $g(\gamma(t))$ is a continuous function of t with $g(\gamma(t)) \in \{1, -1\}$ and $g(\gamma(0)) = 1$; the only possibility is $g(\gamma(1)) = 1$ by continuity). Since $SU(2)$ is connected, then all $U \in SU(2)$ can be reached by continuous path from I, hence $g(U) = 1$ for all $U \in SU(2)$, hence $\det(R_U) = 1$ for all $U \in SU(2)$ hence $R_U \in SO(3)$.

We have shown that $R_U \in SO(3)$. Hence, we have a map $\varphi : SU(2) \to SO(3)$ given by

$$\varphi(U) = R_U.$$

We now want to show that φ is a homomorphism. We have

$$\Theta^{-1}(R_{U_1U_2}(\boldsymbol{b})) = \Phi_{U_1U_2}(\Theta^{-1}(\boldsymbol{b})) = U_1U_2\Theta^{-1}(\boldsymbol{b})U_2^\dagger U_1^\dagger = \Phi_{U_1}(\Phi_{U_2}(\Theta^{-1}(\boldsymbol{b})))$$

hence

$$\varphi(U_1U_2) = R_{U_1U_2} = \Theta\circ\Theta^{-1}\circ R_{U_1U_2} = \Theta\circ\Phi_{U_1}\circ\Phi_{U_2}\circ\Theta^{-1} = \Theta\circ\Phi_{U_1}\circ\Theta^{-1}\circ\Theta\circ\Phi_{U_2}\circ\Theta^{-1} = R_{U_1}\circ R_{U_2}$$

which is the homomorphism property.

Then, we would have to prove that φ is onto – this requires more precise calculation of what φ is as function of the matrix elements of U. We will omit this step.

Finally, we can use the homomorphism theorem. We must calculate $\ker\varphi$. The identity in $O(3)$ is the identity matrix. We have $\varphi(U) = I \in O(3)$ iff $\Theta(\Phi_U(\Theta^{-1}(\boldsymbol{b}))) = \boldsymbol{b}$ for all $\boldsymbol{b} \in \mathbb{R}^3$, which is true iff $\Phi_U(\boldsymbol{b}\cdot\boldsymbol{\sigma}) = \boldsymbol{b}\cdot\boldsymbol{\sigma}$ for all $\boldsymbol{b} \in \mathbb{R}^3$, which is true iff $U\boldsymbol{b}\cdot\boldsymbol{\sigma}U^\dagger = \boldsymbol{b}\cdot\boldsymbol{\sigma} \Leftrightarrow U\boldsymbol{b}\cdot\boldsymbol{\sigma} = \boldsymbol{b}\cdot\boldsymbol{\sigma}U \Leftrightarrow U\sigma_i = \sigma_i U^\dagger$ for $i = 1, 2, 3$. Since also $UI = IU$, we then have that $\varphi(U) = I \in O(3)$ iff $U(aI + \boldsymbol{b}\cdot\boldsymbol{\sigma}) = (aI + \boldsymbol{b}\cdot\boldsymbol{\sigma})U$ for all $a, b_x, b_y, b_z \in \mathbb{C}$. Hence, iff $UA = AU$ for all $A \in M_2(\mathbb{C})$. This only holds if $U = cI$ for some $c \in \mathbb{C}$. Since we must have $U \in SU(2)$, then $|c|^2 = 1$ and $\det(U) = c^2 = 1$ so that $c = \pm 1$. Hence, $\ker\varphi = \{I, -I\} \subset SU(2)$. Clearly, $\{I, -I\} \cong \mathbb{Z}_2$. This completes the sketch proof of the theorem. □

14. The Semi-Direct Product

The semi-direct product is a generalisation of the direct product. Take two groups G and H and consider the Cartesian product of these sets $G \times H = \{(g,h) : g \in G,\ \ h \in H\}$. This new set can be given the structure of a group simply by taking the multiplication law $(g,h)(g',h') = (gg', hh')$. But there is another way of defining a multiplication law on the same set, leading to a (generically) different group structure.

Let's recall some properties of the direct product $J = G \times H$:

- Its elements are the Cartesian product of elements of G and H, i.e. $(g,h) \in G \times H$ for $g \in G$ and $h \in H$.

- The subset $(G,e) = \{(g,e) : \forall g \in G\}$ is isomorphic to G, under the isomorphism $\phi((g,e)) = g$, and the subset $(e,H) = \{(e,h) : \forall h \in H\}$ is isomorphic to H.

- $G \cong (G,e)$ is a normal subgroup of $J = G \times H$ as

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

  Similarly $H \cong (e,H)$ is a normal subgroup of J. Both G and H are normal subgroups of J.

- $(g,e)(e,h) = (ge, eh) = (e,h)(g,e)$ i.e. $(G,e)(e,H) = (e,H)(G,e)$ which is equivalent to the statement $GH = HG$ as sets. Expressing $J = GH$ is called the *inner direct product* while the method we have adopted of using the Cartesian product to express elements of J is also known as the *exterior direct product.*

- Note that $(G,e) \cap (e,H) = (e,e)$, the identity element in $J = G \times H$ i.e. $G \cap H = \{e\}$.

Example 14.1.

- *$\mathbb{Z}_2 \times \mathbb{Z}_3$. Consider $\mathbb{Z}_2$ with generating element a and $\mathbb{Z}_3$ with generating element b, then*

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(e,e) \equiv E, (a,e) \equiv A, (e,b) \equiv B, (a,b) \equiv AB, (e,b^2) \equiv B^2, (a,b^2) \equiv AB^2\}.$$

Now as elements of the direct-product group we have

$$\mathbb{Z}_2 = \{E, A\} \qquad \text{and} \qquad \mathbb{Z}_3 = \{E, B, B^2\}$$

so that the product of $\mathbb{Z}_2$ and $\mathbb{Z}_3$ as sets is

$$\mathbb{Z}_2\mathbb{Z}_3 = \{EE, EB, EB^2, AE, AB, AB^2\} = \{E, B, B^2, A, AB, AB^2\} = \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Further because of the normality of the subgroups $\mathbb{Z}_2$ and $\mathbb{Z}_3$ we have $\mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_2\mathbb{Z}_3 = \mathbb{Z}_3\mathbb{Z}_2$.

- *The direct product and quotient groups: For $J = G \times H$ consider the map $\phi : J \to H$ given by $\phi((g,h)) = h$. It is a homomorphism as $\phi((g_1,h_1))\phi((g_2,h_2)) = h_1h_2$ and $\phi((g_1,h_1)(g_2,h_2)) = \phi((g_1g_2,h_1h_2)) = h_1h_2$, so ϕ is a homomorphism. As $\ker(\phi) = (G,e) \cong G$ then by the homomorphism theorem we have*

$$\frac{J}{\ker\phi} \cong \frac{G \times H}{G} \cong H.$$

Via a similar homomorphism $\psi : J \to G$ as $\psi((g,h)) = g$ we can also show that

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

Let us weaken the properties of the direct product slightly to construct the semi-direct product: instead of both G and H being normal subgroups of J we will require only that H is a normal subgroup.

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 is a normal subgroup of J and*

(iii) $H \cap G = \{e\}$.

The semi-direct product is denoted $J = G \ltimes H$.

Comment(s). *(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. *Notation: $J \triangleright H$ denotes that H is a normal subgroup of J, and the notation for a semi-direct product ($\ltimes$) is a mixture of the symbol for a direct product ($\times$) and the symbol for a normal subgroup ($\triangleright$). Hence $G \ltimes H$ encodes the fact that the semi-direct product can act on the set $G \times H$ and further that H is a normal subgroup of $G \ltimes H$.*

3. *As H is normal then $hg = (gg^{-1})hg = g((g^{-1})h(g^{-1})^{-1}) = gh'$. Therefore $HG = GH$ as sets.*

4. *For the semi-direct product $J = HG$ we can construct the homomorphism $\phi(hg) = g$ as $\phi(h_1g_1)\phi(h_2g_2) = g_1g_2$ while $\phi(h_1g_1h_2g_2) = \phi(h_1g_1h_2g_1^{-1}g_1g_2) = \phi(h_1h_2'g_1g_2) = g_1g_2$. Via the homomorphism theorem we then have $\frac{J}{H} \cong G$. On the other hand $\psi : J \to H$ given by $\psi(hg) = h$ is not a homomorphism as $\psi(h_1g_1)\psi(h_2g_2) = h_1h_2$ while $\psi(h_1g_1h_2g_2) = \psi(h_1g_1h_2g_1^{-1}g_1g_2) = \psi(h_1h_2'g_1g_2) = h_1h_2'$.*

5. *J is called the extension of H by G.*

6. *Consider multiplying two elements in $J = HG$:*

$$(h_1g_1)(h_2g_2) = h_1g_1h_2g_1^{-1}g_1g_2 = h_1h_2'g_1g_2 \in HG.$$

By using the fact that H is a normal subgroup in J we have a group product on J that satisfies the closure axiom of a group. In the following definition we will write a general element of $J = HG$ as an element of the set $G \times H$ as $hg \to (g, h)$. In this notation the product above is written

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2') = (g_1g_2, h_1g_1h_2g_1^{-1}).$$

Example 14.2. *Consider $\frac{GL(N,\mathbb{R})}{SL(N,\mathbb{R})} \cong \mathbb{R}^*$. This isomorphism indicates that we could take $H = SL(N, \mathbb{R})$ (a normal subgroup of $GL(N, \mathbb{R})$) and construct $GL(N, \mathbb{R})$ as the extension of $H = SL(N, \mathbb{R})$ by $G = \mathbb{R}^*$. However we will see that there are some obstructions to the naive construction of the the whole of $GL(N, \mathbb{R})$ in this example.*

- *$N = 2$: Let $A \in SL(2, \mathbb{R})$ and $\lambda \in \mathbb{R}^*$ then we can construct the matrix $A\lambda = \lambda A$ by multiplying all four entries of A by λ using multiplication on $\mathbb{R}$. We find that $\det(\lambda A) = \lambda^2 \det(A) = \lambda^2 \in \mathbb{R}^+$. Hence by this method we have only constructed the subset of matrices of $GL(2, \mathbb{R})$ which have positive determinant.*

- $N = 3$*: As above but now let* $A \in SL(3, \mathbb{R})$ *and consider the matrix* λA *which satisfies* $\det(\lambda A) = \lambda^3 \in \mathbb{R}^*$*. Hence* $\lambda A \in GL(3, \mathbb{R})$ *and further we can show that any matrix in* $GL(3, \mathbb{R})$ *can be expressed in the form* λA *where* $\lambda \in \mathbb{R}^*$ *and* $A \in SL(3, \mathbb{R})$*.*

We will now construct the semi-direct product group via an explicit action on the set $G \times H$, which has been indicated in the comments above.

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*

$$(g, h)(g', h') = (gg', h\phi_g(h')). \tag{14.1}$$

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

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

Proof. We check the axioms of a group:

- Closure: $gg' \in G$ 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:

  $$(g, h)((g', h')(g'', h'')) = (g, h)(g'g'', h'\phi_{g'}(h'')) = (gg'g'', h\phi_g(h'\phi_{g'}(h''))).$$

  The second member in the last term can be written $h\phi_g(h')\phi_g(\phi_{g'}(h''))$ (because ϕ_g is a homomorphism of H) and then $= h\phi_g(h')\phi_{gg'}(h'')$ (because ϕ is a homomorphism). On the other hand,

  $$((g, h)(g', h'))(g'', h'') = (gg', h\phi_g(h'))(g'', h'') = (gg'g'', h\phi_g(h')\phi_{gg'}(h''))$$

  which is in agreement with the previous result.

- Identity: (e, e) is the identity element as

  $$(e, e)(g, h) = (eg, e\phi_e(h)) = (g, ehe^{-1}) = (g, h).$$

  This follows as $\phi_e = \mathrm{id}$, the identity map in $\mathrm{Inn}(H)$. Also,

  $$(g, h)(e, e) = (ge, h\phi_g(e)) = (g, he) = (g, h)$$

  as $\phi_g(e) = e$ for all $g \in G$ (because ϕ_g is a homomorphism).

- Inverses: The inverse element to (g,h) is given by

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

  because we have

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

  and

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

□

Comment(s). *(On the $G \ltimes H$ multiplication law.)*

1. *$H \cong (e,H)$ is a normal subgroup of $J = G \ltimes H$ under this group multiplication law as*

   $$\begin{aligned}(g,h')(e,h)(g,h')^{-1} &= (g,h')(e,h)(g^{-1}, \phi_{g^{-1}}(h'^{-1}))\\ &= (g,h')(eg^{-1}, h\phi_e(\phi_{g^{-1}}(h'^{-1})))\\ &= (g,h')(g^{-1}, h\phi_{g^{-1}}(h'^{-1}))\\ &= (e, h'\phi_g(h\phi_{g^{-1}}(h'^{-1})))\\ &\in (e,H)\end{aligned}$$

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

2. *By mapping $(g,e) \to g$ and $(e,h) \to h$ we may reconstruct $G \ltimes H$ as HG using the product defined above:*

   $$(e,h)(g,e) = (g, h\phi_e(e)) = (g,h)$$

   for all $g \in G$, $h \in H$. Note that

   $$(g,h) = (g,e)(e,h') = (g, e\phi_g(h')) = (g, gh'g^{-1})$$

   hence $h' = \phi_{g^{-1}}(h)$. So we have $(G,e)(e,H) = (e,H)(G,e)$.

3. *Note that as $G \cong (G,e)$ and $H \cong (e,H)$ then $G \cap H = \{(e,e)\}$ the identity element in $G \ltimes H$.*

4. *Due to the above comments we see that this construction of the semi-direct product on the set $G \times H$ with the multiplication law given in equation (14.1), is equivalent to the definition of the semi-direct product group in Definition 14.1.*

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

Theorem 14.2.

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

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

Proof. It is helpful to write the elements of $\mathbb{Z}_2$ as $N \times N$ matrices. Explicitly we will use $\mathbb{Z}_2 = \{I, R\}$ where I is the $N \times N$ identity matrix and R (for reflection) is the matrix

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

Indeed $R^2 = I$ and you may check that $\{I, R\}$ is a subgroup of $O(N)$ isomorphic to $\mathbb{Z}_2$.

1. We first show that $\psi : \mathbb{Z}_2 \to \mathrm{Aut}(SO(N))$ is a homomorphism and is well-defined i.e. that ψ really maps into automorphisms of $SO(N)$: $\varphi_s \in \mathrm{Aut}(SO(N))$ for all $s \in \mathbb{Z}_2$.

   (a) We check that φ_s is an automorphism of $SO(N)$ for any s. Let us fix $s \in \mathbb{Z}_2$. First φ_s maps $SO(N)$ into $SO(N)$. Indeed, both I and R are in $O(N)$, hence if $g \in SO(N)$, then $\varphi_s(g) = sgs \in O(N)$ by closure in $O(N)$; and further, still with $g \in SO(N)$, we have $\det(sgs) = \det(s)^2 \det(g) = 1$; so that $\varphi_s(g) \in SO(N)$. Second, φ_s is onto $SO(N)$. Indeed, for every $g \in SO(N)$, we have $sgs \in SO(N)$ as said, and we find $\varphi_s(sgs) = s^2gs^2 = g$. Third, φ_s is injective. Indeed $\varphi_s(g) = \varphi_s(g') \Rightarrow sgs = sg's \to g = g'$ by left and right multiplication by s. Finally, φ_s is a homomorphism. Indeed, $\varphi_s(gg') = sgg's = sgssg's = \varphi_s(g)\varphi_s(g')$ where we used $s^2 = I$, which holds both for $s = I$ and $s = R$. Hence φ_s is a bijective automorphism of $SO(N)$ onto $SO(N)$: it is in $\mathrm{Aut}(SO(N))$.

   (b) Then, we show that ψ is a homomorphism. Indeed, $\psi(s)\psi(s') = \varphi_s \circ \varphi_{s'}$, and in order to see what map this is we act on an arbitrary element $g \in SO(N)$: $(\varphi_s \circ \varphi_{s'})(g) = ss'gs's = ss'gss' = \varphi_{ss'}(g)$. Hence we find $\varphi_s \circ \varphi_{s'} = \varphi_{ss'} = \psi(ss')$.

2. Now we construct an isomorphism ϕ that maps $O(N)$ onto $\mathbb{Z}_2 \ltimes_\psi SO(N)$. Here, for convenience, we use the following notation: we define $\omega : O(N) \to \{I, R\}$ as $\omega(A) = I$ if

$\det(A) = 1$ and $\omega(A) = R$ if $\det(A) = -1$. It is easy to check that ω is a homomorphism: $\omega(AB) = \omega(A)\omega(B)$. We then define ϕ as

$$\begin{aligned} \phi \;\; : \;\; & O(N) \to \mathbb{Z}_2 \ltimes SO(N) \\ & A \mapsto \phi(A) = (\omega(A), A\,\omega(A)) \end{aligned}$$

Again all we have to show is that this maps into the right space as specified (because this is not immediately obvious), and then that it is indeed an isomorphism.

First: that it maps into $\mathbb{Z}_2 \times SO(N)$ is shown as follows. a) Clearly $\omega(A) \in \mathbb{Z}_2$. b) Also $\omega(A)$ and A are in $O(N)$ hence $A\omega(A) \in O(N)$. Further, $\det(A\omega(A)) = \det(A)\det(\omega(A)) = \det(A)^2 = 1$. Hence indeed $A\,\omega(A) \in SO(N)$.

Second: that it is a homomorphism:

$$\begin{aligned} \phi(A)\phi(B) &= (\omega(A), A\omega(A))\,(\omega(B), B\omega(B)) \\ &= \big(\omega(A)\omega(B), A\omega(A)\varphi_{\omega(A)}(B\omega(B))\big) \\ &= (\omega(AB), A\omega(A)\omega(A)B\omega(B)\omega(A)) \\ &= (\omega(AB), AB\omega(A)\omega(B))) \\ &= (\omega(AB), AB\omega(AB)) \\ &= \phi(AB) \end{aligned}$$

Third: that it is bijective. Injectivity: if $\phi(A_1) = \phi(A_2)$ then $\omega(A_1) = \omega(A_2)$ and $A_1\omega(A_1) = A_2\omega(A_2)$, combining these we find $A_1 = A_2$ so indeed it is injective. Surjectivity: take $s \in \mathbb{Z}_2$ and $B \in SO(N)$. We can always find a matrix $A \in O(N)$ such that $\phi(A) = (s, B)$. Indeed, just take $A = Bs$. Since both B and s are in $O(N)$, then also is Bs. Also, we have $\omega(A) = \omega(B)\omega(s) = \omega(B)s = s$ where we used that $\omega(s) = s$ for any $s \in \{I, R\}$, and that $\omega(B) = I$ because $\det(B) = 1$. Further, $A\omega(s) = Bs^2 = B$. Hence, $\phi(A) = (\omega(A), A\omega(s)) = (s, B)$ as it should.

□

The semi-direct product decomposition makes very clear the structures involved in the quotient, e.g. $O(N)/SO(N) \cong \mathbb{Z}_2$. This is a general phenomenon:

Theorem 14.3. *The subset $\{(e, h) : h \in H\} \subset G \times H$ is a subgroup of $G \ltimes_\psi H$ that is isomorphic to H and that is normal. The subset $\{(g, e) : g \in G\}$ is a subgroup of $G \ltimes_\psi H$ that is isomorphic to G.*

Proof. For the first statement: it is a subgroup because it contains the identity (e, e), it is closed $(e, h)(e, h') = (e, h\varphi_e(h')) = (e, hh')$, and it contains the inverse, $(e, h)^{-1} = (e, h^{-1})$ by the multiplication rule just established. It is also clearly isomorphic to H, with $(e, h) \mapsto h$, thanks again to the multiplication rule. Further, it is normal:

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

For the second statement, the subset contains the identity, is closed $(g, e)(g', e) = (gg', \varphi_g(e)) = (gg', e)$, and by this multiplication law, it contains the inverse. Clearly again, it is isomorphic to G. □

A special case of the semi-direct product is the direct product, where $\varphi_g = \mathrm{id}$ for all $g \in G$ (that is, $\psi : G \to \mathrm{Aut}(H)$ is trivial, $\psi(g) = \mathrm{id}$). In this case, both G and H are normal subgroups.

Theorem 14.4. *The left cosets of $G \ltimes H$ with respect to the normal subgroup H are the subsets $\{(g, h) : h \in H\}$ for all $g \in G$. Also, $(G \ltimes H)/H \cong G$.*

Proof. For the first statement: the left cosets are $(g, h)(e, H) = (g, h\varphi_g(H)) = (g, hH) = (g, H)$. In the second equality we used that φ_g is an automorphism, and in the third we used that the left multiplication by h is a bijection of H (show this!). For the second statement: the isomorphism is $(g, H) \mapsto g$. This is clearly bijective, and it is a homomorphism, because $(g, H)(g', H) = (gg', H\varphi_g(H)) = (gg', H)$. □

Note also that the right cosets are the same: $(e, H)(g, h) = (g, H\varphi_e(h)) = (g, Hh) = (g, H)$. Hence we also have $H\backslash(G \ltimes H) \cong G$.

Coming back to our example: $SO(N)$ is indeed a normal subgroup of $O(N) \cong \mathbb{Z}_2 \ltimes SO(N)$, but the $\mathbb{Z}_2$ of this decomposition, although it is a subgroup, is not normal. The $\mathbb{Z}_2$ of this decomposition can be obtained as an explicit subgroup of $O(N)$ by the inverse map ϕ^{-1} of Theorem 14.2: $\phi^{-1}((s, I)) = s$ (recall that $s \in \{I, R\}$). Hence the subgroup is $\{I, \mathrm{diag}(-1, 1, \ldots, 1)\}$. Here, we indeed have that $SO(N)$ is the kernel of det, and that $\{I, R\}$ is a subgroup on which det is an isomorphism.

Note: Clearly, there are many $\mathbb{Z}_2$ subgroups, for instance $\{I, -I\}$; this one is normal. But for N even, it does not take part into any decomposition of $O(N)$ into $\mathbb{Z}_2$ and $SO(N)$.

15. The Euclidean Group

The Euclidean group is the group of transformations of the Euclidean plane, $\mathbb{R}^N$, which leaves the distance between any two points invariant. The distance function on $\mathbb{R}^N$ can be defined explicitly using the Euclidean inner product:

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

In this chapter we will prove that *all* the transformations which preserve the Euclidean inner product are formed of just the orthogonal transformations and the translations of $\mathbb{R}^N$. Furthermore we will show that the Euclidean group is a semi-direct product group of $O(N)$ and $\mathbb{R}^N$ the (abelian) group of real vectors in $\mathbb{R}^N$ under addition.

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

Proof. The set of all translations of $\mathbb{R}^N$ is the set of all maps $\boldsymbol{x} \mapsto \boldsymbol{x} + \boldsymbol{b}$ for $\boldsymbol{b} \in \mathbb{R}^N$: maps that take each point $\boldsymbol{x}$ to $\boldsymbol{x} + \boldsymbol{b}$ in $\mathbb{R}^N$. Let us denote a translation by $T_{\boldsymbol{b}}$, so that $T_{\boldsymbol{b}}(\boldsymbol{x}) = \boldsymbol{x} + \boldsymbol{b}$. The composition law is obtained from

$$(T_{\boldsymbol{b}} \circ T_{\boldsymbol{b}'})\boldsymbol{x} = T_{\boldsymbol{b}}(T_{\boldsymbol{b}'})\boldsymbol{x} = T_{\boldsymbol{b}}(\boldsymbol{x} + \boldsymbol{b}') = \boldsymbol{x} + \boldsymbol{b} + \boldsymbol{b}' = T_{\boldsymbol{b}+\boldsymbol{b}'}(\boldsymbol{x}).$$

Hence, $T_{\boldsymbol{b}} \circ T_{\boldsymbol{b}'} = T_{\boldsymbol{b}+\boldsymbol{b}'}$, so that compositions of translations are translations. Further, there is an identity translation that does nothing (choosing $\boldsymbol{b} = \boldsymbol{0}$). An inverse translation always exists: $T_{\boldsymbol{b}} \circ T_{-\boldsymbol{b}} = T_{\boldsymbol{0}} = \text{id}$. Hence, the set of all translations, with multiplication law the composition of maps, is a group. Note also that $T_{\boldsymbol{b}} \neq T_{\boldsymbol{b}'}$ if $\boldsymbol{b} \neq \boldsymbol{b}'$ and for any $\boldsymbol{b} \in \mathbb{R}^N$ there is a $T_{\boldsymbol{b}}$. Clearly, then, this is a group that is isomorphic to $\mathbb{R}^N$, by the map

$$T_{\boldsymbol{b}} \mapsto \boldsymbol{b}.$$

□

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

Proof. We have that $Q : \mathbb{R}^N \to \mathbb{R}^N$ and that $D(Q(\boldsymbol{x}), Q(\boldsymbol{y})) = D(\boldsymbol{x}, \boldsymbol{y})$. Suppose, without loss of generality, that $Q(\mathbf{0}) = \boldsymbol{b}$ then $Q' \equiv T_{-\boldsymbol{b}} \circ Q$ is a transformation that leaves the origin $\mathbf{0}$ fixed as $Q'(\mathbf{0}) = T_{-\boldsymbol{b}} \circ Q(\mathbf{0}) = T_{-\boldsymbol{b}}\boldsymbol{b} = \mathbf{0}$. We note that translations of $\mathbb{R}^N$ by any vector $-\boldsymbol{b} \in \mathbb{R}^N$ preserve the distance as $D(\boldsymbol{x} - \boldsymbol{b}, \boldsymbol{y} - \boldsymbol{b}) = ||\boldsymbol{x} - \boldsymbol{y}|| = D(\boldsymbol{x}, \boldsymbol{y})$. In particular Q' also preserves the distance i.e. $D(Q'(\boldsymbol{x}), Q'(\boldsymbol{y})) = D(Q(\boldsymbol{x}), Q(\boldsymbol{y})) = D(\boldsymbol{x}, \boldsymbol{y})$ as Q preserves the inner product by assumption.

Now let us show that not only does Q' preserve the distance function it also preserves the inner product by using $D(Q'(\boldsymbol{x}), Q'(\boldsymbol{y})) = D(\boldsymbol{x}, \boldsymbol{y})$. Let us square this expression in terms of inner products (to remove the square root for convenience) it becomes

$$(Q'(\boldsymbol{x}) - Q'(\boldsymbol{y}), Q'(\boldsymbol{x}) - Q'(\boldsymbol{y})) = (\boldsymbol{x} - \boldsymbol{y}, \boldsymbol{x} - \boldsymbol{y})$$

Using the bilinearity of the inner product we can expand this to

$$(Q'(\boldsymbol{x}), Q'(\boldsymbol{x})) - 2(Q'(\boldsymbol{x}), Q'(\boldsymbol{y})) + (Q'(\boldsymbol{y}), Q'(\boldsymbol{y})) = (\boldsymbol{x}, \boldsymbol{x}) - 2(\boldsymbol{x}, \boldsymbol{y}) + (\boldsymbol{y}, \boldsymbol{y}). \tag{15.1}$$

Of course we are tempted to conclude that $(Q'(\boldsymbol{x}), Q'(\boldsymbol{y})) = (\boldsymbol{x}, \boldsymbol{y})$, but we must take care to prove this. We know that $D(Q'(\boldsymbol{x}), \mathbf{0}) = \sqrt{(Q'(\boldsymbol{x}), Q'(\boldsymbol{x}))}$ and we can write out the left-hand-side of this expression in terms of Q:

$$\begin{aligned} D(Q'(\boldsymbol{x}), \mathbf{0}) &= D(T_{-\boldsymbol{b}}Q(\boldsymbol{x}), \mathbf{0}) \\ &= D(Q(\boldsymbol{x}), T_{\boldsymbol{b}}\mathbf{0}) \\ &= D(Q(\boldsymbol{x}), \boldsymbol{b}) \\ &= D(Q(\boldsymbol{x}), Q(\mathbf{0})) \\ &= D(\boldsymbol{x}, \mathbf{0}) \\ &= \sqrt{(\boldsymbol{x}, \boldsymbol{x})}. \end{aligned}$$

Hence we have that $(Q'(\boldsymbol{x}), Q'(\boldsymbol{x})) = (\boldsymbol{x}, \boldsymbol{x})$ and so also $(Q'(\boldsymbol{y}), Q'(\boldsymbol{y})) = (\boldsymbol{y}, \boldsymbol{y})$ which we may substitute into equation (15.1) to obtain

$$(Q'(\boldsymbol{x}), Q'(\boldsymbol{y})) = (\boldsymbol{x}, \boldsymbol{y})$$

so we have shown that Q' is a transformation that preserves the inner product.

Now we show that Q' is a linear transformation. Let $\boldsymbol{e}_i$, $i = 1, 2, \ldots, N$ be orthonormal vectors in $\mathbb{R}^N$ (this is the standard basis for $\mathbb{R}^N$ as a vector space). Let $\boldsymbol{e}'_i := Q'(\boldsymbol{e}_i)$ then since Q' preserves the inner product $\boldsymbol{e}'_i$ form another orthonormal basis of $\mathbb{R}^N$. Now let $\boldsymbol{x} = \sum_i x_i\boldsymbol{e}_i$ for $x_i \in \mathbb{R}$, then $Q'(\boldsymbol{x}) \equiv \sum_i x'_i\boldsymbol{e}'_i$ (this can be done because $\boldsymbol{e}'_i$ form a basis). We can find x'_i by taking inner products with $\boldsymbol{e}'_i$:

$$\begin{aligned} x'_i &= (Q'(\boldsymbol{x}), \boldsymbol{e}'_i) \qquad\qquad \text{as } (\boldsymbol{e}_i, \boldsymbol{e}_j) = \delta_{ij} \\ &= (Q'(\boldsymbol{x}), Q'(\boldsymbol{e}_i)) \\ &= (\boldsymbol{x}, \boldsymbol{e}_i) \\ &= x_i \end{aligned}$$

Therefore $Q'(\boldsymbol{x}) = \sum_i x_i \boldsymbol{e}'_i$ which implies that Q' is a linear transformation (as the components of $\boldsymbol{x}$ appear linearly in $Q'(\boldsymbol{x})$). Hence, we have found that Q' is a linear transformation which preserves length of vectors in $\mathbb{R}^N$, so it must be in $O(N)$. Hence, $Q = T_{\boldsymbol{b}} \circ Q' \equiv T_{\boldsymbol{b}} \circ A$ where $A \in O(N)$, so that Q is a map constructed from a translation and an orthogonal transformation. □

We will now show that the Euclidean group is a semi-direct product group:

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

To confirm that the Euclidean group is well-defined we should show that ψ is a homomorphism and that φ is an automorphism.

First, we show that φ is an automorphism: φ_A is clearly bijective because the matrix A is invertible. Further, it is a homomorphism because $\varphi_A(\boldsymbol{x} + \boldsymbol{y}) = A(\boldsymbol{x} + \boldsymbol{y}) = A\boldsymbol{x} + A\boldsymbol{y} = \varphi_A(\boldsymbol{x}) + \varphi_A(\boldsymbol{y})$. Second, we show that ψ is a homomorphism: as $\varphi_{AA'}(\boldsymbol{b}) = AA'\boldsymbol{b} = A(A'\boldsymbol{b}) = \varphi_A(\varphi_{A'}(\boldsymbol{b})) = (\varphi_A \circ \varphi_{A'})(\boldsymbol{b})$ so that $\psi(AA') = \psi(A)\psi(A')$ (the group multiplication law for automorphisms is the composition of maps). Hence the semi-direct product in the definition of the Euclidean group is well-defined.

A general element of the Euclidean group will consist of both an orthogonal transformation A and a translation $T_{\boldsymbol{b}}$ which we will denote as $(A, T_{\boldsymbol{b}}) = T_{\boldsymbol{b}} \circ A$ i.e.

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

Then, let us see what happens when we compose such transformations. We have

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

That is, we obtain a transformation that can be described by first an orthogonal transformation AA', then a translation by the vector $A\boldsymbol{b}' + \boldsymbol{b}$. Combined with the definition of the Euclidean group above and the fact that $T_{\boldsymbol{b}} \mapsto \boldsymbol{b}$ is an isomorphism, what we have just shown is that the set of all transformations "orthogonal transformations followed by translation" is the same set as the set E_N. That is, the Euclidean group can be seen as the group of such transformations.

Furthermore the composition law for orthogonal transformations followed by a translation is the same as that of $O(N) \ltimes_{\psi} \mathbb{R}^N$, and the two groups of transformations are isomorphic. Note how the semi-direct multiplication law occurs essentially because orthogonal transformations and translations don't commute:

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

so that $T_{\boldsymbol{b}} \circ A \circ T_{\boldsymbol{b}'} \circ A' \neq T_{\boldsymbol{b}} \circ T_{\boldsymbol{b}'} \circ A \circ A'$. We rather have $T_{\boldsymbol{b}} \circ A \circ T_{\boldsymbol{b}'} \circ A' = T_{\boldsymbol{b}} \circ A \circ T_{\boldsymbol{b}'} \circ A^{-1} \circ A \circ A'$, and we find the conjugation law

$$A \circ T_{\boldsymbol{b}'} \circ A^{-1}(\boldsymbol{x}) = A(A^{-1}\boldsymbol{x} + \boldsymbol{b}') = \boldsymbol{x} + A\boldsymbol{b}' = T_{A\boldsymbol{b}'}(\boldsymbol{x})$$

That is: the conjugation of a translation $T_{\boldsymbol{b}'}$ by an orthogonal transformation A is again a translation, but by the rotated/reflected vector, $T_{A\boldsymbol{b}'}$ and this is what gives rise to the semi-direct product law. This is true generally: if two type of transformations don't commute, but the conjugation of one by another is again of the first type, then we have a semi-direct product. Recall also examples of $SO(2)$ and $\mathbb{Z}_2$ in their geometric interpretation as rotations and reflections.

There is more. We could decide to try to do translations and orthogonal transformations in any order – that is, we can look at all transformations of $\mathbb{R}^N$ that are obtained by doing orthogonal transformations and translations in any order and of any kind. A general transformation will look like $A_1 \circ A_2 \circ \cdots \circ T_{\boldsymbol{b}_1} \circ T_{\boldsymbol{b}_2} \circ \cdots \circ A'_1 \circ A'_2 \circ \cdots$ etc. But since orthogonal transformations and translations independently form groups, we can multiply successive orthogonal transformations to get a single one, and like wise for translations, so we get something of the form $A \circ T_{\boldsymbol{b}} \circ A' \circ \ldots$ etc. Further taking into account that we can always put the identity orthogonal transformation at the beginning, and the identity translation at the end, if need be, we always recover something of the form $(A, T_{\boldsymbol{b}})(A', T_{\boldsymbol{b}'}) \cdots$. Hence, we recover a Euclidean transformation. Hence, the Euclidean group is the one generated by translations and orthogonal transformations. We have proved:

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

Comment(s). *(On the Poincaré group.) The Euclidean group arose from studying the transformations which leave the Euclidean distance invariant. If we had considered the transformations which leave an alternative distance function unchanged we would find another group. The Minkowski metric is important in physics and is used to measure distance in a four-dimensional space-time $\mathbb{R}^4$. Let us work in four dimensions, and denote the components of a vector $\boldsymbol{x}$ by x^μ for $\mu = 0, 1, 2, 3$ (standard notation in physics, from Einstein). Then the Minkowski metric on $\mathbb{R}^4$ is*

$$< \boldsymbol{x}, \boldsymbol{y} >_M \equiv \sum_{\mu\nu=0}^{3} \eta_{\mu\nu} x^\mu y^\nu, \quad \eta_{\mu\nu} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{15.2}$$

The quantity $\eta_{\mu\nu}$ is called the Minkowski metric. Note that $< \boldsymbol{x}, \boldsymbol{x} >_M = -(x_0)^2 + (x_1)^2 + (x_2)^2 + (x_3)^2$ so that the length-squared of a vector could be negative, zero or positive.

Due to the many repeated sums appearing when using the Minkowski metric it is convenient to adopt Einstein's summation convention. There is no ambiguity over which indices are being summed over as they are repeated, hence we do not need to write the summation symbol $\sum_{\mu,\nu=0}^{3}$ as it a summation over an index is automatically implied whenever there is the index somewhere at the bottom (like μ or ν in $\eta_{\mu\nu}$) and the same index somewhere else at the top (like μ in x^μ) in the same term. With this convention we would write $< \boldsymbol{x}, \boldsymbol{y} >_M = \eta_{\mu\nu} x^\mu y^\nu$ with the summation over the repeated indices being implied.

Definition 15.2. *The Poincaré group is the group of transformations that keep invariant the distance measured in $\mathbb{R}^4$ using the Minkowski inner product.*

This is an invariance definition for the Poincaré group. In much the same way that we showed that the invariance definition of the Euclidean group is equivalent to a semi-direct product definition ($O(N) \ltimes \mathbb{R}^N$), there is also something similar for the Poincaré group. Except now, instead of rotations and reflections $O(N)$ we have Lorentz transformations *L.*

Definition 15.3. *A Lorentz transformation $\Lambda \in L$ is a linear map on $\mathbb{R}^4$ which preserves the Minkowski inner product:*

$$< \Lambda \boldsymbol{x}, \Lambda \boldsymbol{y} >_M = < \boldsymbol{x}, \boldsymbol{y} >_M . \tag{15.3}$$

Let us rewrite this condition in components.

$$\Lambda^\mu{}_\kappa x^\kappa \Lambda^\nu{}_\lambda y^\lambda \eta_{\mu\nu} = x^\kappa y^\lambda \eta_{\kappa\lambda}. \tag{15.4}$$

where we are using the Einstein summation convention so that every repeated indices is summed over. This implies

$$\Lambda^\mu{}_\kappa \Lambda^\nu{}_\lambda \eta_{\mu\nu} = \eta_{\kappa\lambda}. \tag{15.5}$$

An analysis of what the Lorentz transformations Λ are exactly as four-by-four matrices is beyond the scope of these lecture notes, but this equation above is the starting point for defining them. We will note here the following theorem, whose proof (omitted) is similar to that of the corresponding theorem for the Euclidean group.

Theorem 15.4. *The Poincaré group is isomorphic to the semi-direct product $L \ltimes_\Psi \mathbb{R}^4$ with the homomorphism $\Psi : L \to \mathrm{Aut}(\mathbb{R}^N)$ given by $\psi(\Lambda) = \varphi_\Lambda$, and the automorphism $\varphi_\Lambda : \mathbb{R}^4 \to \mathbb{R}^4$ given by $\varphi_\Lambda(\boldsymbol{b}) = \Lambda\boldsymbol{b}$, where $\Lambda \in L$, the Lorentz group.*

16. G-Sets, Stabilisers and Orbits

Groups have an intrinsic action on themselves as a set, but one can allow a group G to act on another set X under certain conditions, e.g. one might allow D_n to act on the Euclidean plane rather than just the n-sided regular polygon P_n. A G-set, X is defined by:

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, and

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

Example 16.1. *$X = G$, the group itself. A group G is a G-set, although there are several standard ways to define the G-set action $g \cdot x$:*

(i) $g \cdot x = gx$ (left multiplication),

(ii) $g \cdot x = xg^{-1}$ (right multiplication - by the inverse element), and

(iii) $g \cdot x = gxg^{-1}$ (conjugation or the Adjoint action).

These actions define G-sets when $X = G$ - this is trivial to see for (i) and (ii) and for (iii) we have for $g_1, g_2, x \in G$

$$
\begin{aligned}
&e \cdot x = exe^{-1} = x \\
&g_1 \cdot (g_2 \cdot x) = g_1 g_2 x g_2^{-1} g_1^{-1} = (g_1 g_2) \cdot x.
\end{aligned}
$$

Example 16.2. *The set of all subsets of G Let X be the set of all subsets of elements of a finite group G. For any subset $S \subset G$ we define the G-set action by $g \cdot S = gS$, i.e. if $S = \{s_1, s_2, \dots s_n\}$ then $g \cdot S = gS = \{gs_1, gs_2, \dots gs_n\} \in X$. The action of left-multiplication by g on a set $S \in X$ produces another set $gS \in X$ containing the same number of elements as S. The axioms of a G-set are satisfied as:*

(i) $e \cdot S = S \quad \forall\, S \in X$, *and*

(ii) $g_1 \cdot (g_2 \cdot S) = g_1 g_2 S = (g_1 g_2) \cdot S \quad \forall\, g_1, g_2 \in G, S \in X$.

Consider the example when $G = \mathbb{Z}_3 = \langle a \rangle$ *with* $a^3 = e$. *The set of all subsets is*

$$X = \{\{\}, \{e\}, \{a\}, \{a^2\}, \{e, a\}, \{e, a^2\}, \{a, a^2\}, \{e, a, a^2\}\}$$

where $\{\}$ *is the empty set* $\emptyset$. *Under the action of* e *all sets are unaltered but under the action of* a *the sets are mapped as follows:*

$$\{\} \xrightarrow{a} \{\}$$

$$\{e\} \xrightarrow{a} \{a\} \xrightarrow{a} \{a^2\} \xrightarrow{a} \{e\}$$

$$\{e, a\} \xrightarrow{a} \{a, a^2\} \xrightarrow{a} \{e, a^2\} \xrightarrow{a} \{e, a\}$$

$$\{e, a, a^2\} \xrightarrow{a} \{e, a, a^2\}$$

and under the action of a^2 *the sets are mapped in the opposite direction compare to* a. *Note that the action moves through all the sets containing the same number of elements. One can modify this example of a* G*-set by changing the action of* G *on* X *while keeping* X *the set of all subsets of* G. *Important examples of the* G*-set action are when* $g \cdot S = Sg^{-1}$ *(to construct right cosets of each subset* S*) or when* $g \cdot S = gSg^{-1}$ *(conjugation). One may further specialise to consider the case where* X *is just those subsets which are also subgroups of* G, *and in this case the* G*-set action of conjugation will preserve the subgroup structure. Conjugation of subgroups of* G *is a* G*-set as, let* H *be a subgroup of* G *then for* $g_1, g_2 \in G$ *we have*

(i) $e \cdot H = eHe^{-1} = H$, *and*

(ii) $g_1 \cdot (g_2 \cdot H) = g_1 g_2 H g_2^{-1} g_1^{-1} = (g_1 g_2) \cdot H$.

Note that if H *is a subgroup of* G *then so is* gHg^{-1} *for* $g \in G$ *as for* $h_1, h_2 \in H$ *we have* $(gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1} \in gHg^{-1}$; *the identity element* e *is in* gHg^{-1} *as* $e \in H$ *and so* $geg^{-1} = e \in gHg^{-1}$; *as* $h^{-1} \in H$ *then* $gh^{-1}g^{-1} \in gHg^{-1}$ *is the inverse element to* $ghg^{-1} \in gHg^{-1}$; *and associativity of the group multiplication law is inherited from the associative multiplication product of* $H \in G$.

For example, consider the subgroups of the dihedral group D_3 *(*$\langle a, b \rangle$ *with* $a^3 = e$, $b^2 = e$ *and* $ab = ba^2$*), the subgroups are:*

$$X = \{\{e\}, \{e, b\}, \{e, ab\}, \{e, a^2b\}, \{e, a, a^2\}, \{e, a, a^2, b, ab, a^2b\}\}.$$

Now under the conjugate action with a *we find the subgroups are mapped as:*

$$\{e\} \xrightarrow{a} \{e\}$$

$$\{e, b\} \xrightarrow{a} \{e, a^2b\} \xrightarrow{a} \{e, ab\} \xrightarrow{a} \{e, b\}$$

$$\{e, a, a^2\} \xrightarrow{a} \{e, a, a^2\}$$

$$\{e, a, a^2, b, ab, a^2b\} \xrightarrow{a} \{e, a, a^2, b, ab, a^2b\}$$

and under conjugation with b:

$$\{e\} \xrightarrow{b} \{e\}$$

$$\{e, b\} \xrightarrow{b} \{e, b\}$$

$$\{e, ab\} \xrightarrow{b} \{e, a^2b\} \xrightarrow{b} \{e, ab\}$$

$$\{e, a, a^2\} \xrightarrow{b} \{e, a, a^2\}$$

$$\{e, a, a^2, b, ab, a^2b\} \xrightarrow{b} \{e, a, a^2, b, ab, a^2b\}$$

and conjugation with all other elements of D_3 consists of successive conjugate actions of a and b.

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

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

Theorem 16.1. *G_x is a subgroup of G.*

Proof. We check that G_x satisfies the defining axioms of a group:

- (Closure) Let $g_1, g_2 \in G_x$ then $(g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x$ so $g_1g_2 \in G_x$.

- (Identity) $e \in G$ is in G_x as $e \cdot x = x$.

- (Inverse) For each $g \in G_x$ then $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$ therefore $g^{-1} \in G_x$.

- (Associativity) Associativity is inherited from the product law of G.

□

Example 16.3. *If $X = G$ and $g \cdot x = gx$ then the stabilisers G_x of each element $g \in X$ are all $\{e\}$, the trivial subgroup.*

Definition 16.3. *Let $X = G$ and $g \cdot x = gxg^{-1}$ then the stabiliser of each element $g \in X$ is called the centraliser of the element $x \in G$:*

$$C_G(x) = \{g \in G \,|\, gxg^{-1} = x\} = \{g \in G \,|\, gx = xg\}.$$

Comment(s). *The centre $Z(G) = \{z \in G \,|\, zg = gz \,\forall\, g \in G\}$ is different from the centraliser of an element $x \in G$. $Z(G)$ consists of all those elements in G which commute with* all *other elements of G, while the centraliser is defined with respect to a single element x, and consists of all those elements of G which commute with x.*

Example 16.4. *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 its order is 1, 2, 3 or 6. But as D_3 is not abelian (e.g. $ab = ba^2$) then $|C_{D_3}(b)| \neq 6$. $C_{D_3}(b)$ contains $\langle b \rangle$ which is a group of order 2, which implies that $|C_{D_3}(b)| = 2$ (as we have ruled out that $|C_{D_3}(b)| = 6$). Hence $C_{D_3}(b) = \langle b \rangle$.

Example 16.5. *We will compute the centralisers of all the elements D_4. As $Z(D_4) = \{e, a^2\}$ then $C_{D_4}(e) = D_4 = C_{D_4}(a^2)$. Now $\langle a \rangle \subset C_{D_4}(a)$ so $|C_{D_4}(a)|$ is either 4 or 8, as D_4 is not abelian then $C_{D_4}(a) = \langle a \rangle = C_{D_4}(a^3)$. Similarly $\langle b \rangle \subset C_{D_4}(b)$ hence $|C_{D_4}(b)| = 2, 4$ however since $a^2 \in Z(D_4)$ then $a^2 \in C_{D_4}(b)$ hence $|C_{D_4}(b)| = 4$ and we find $C_{D_4}(b) = \{e, a^2, b, a^2b\} = C_{D_4}(a^2b)$. Similar arguments lead to $C_{D_4}(ab) = \{e, a^2, ab, a^3b\} = C_{D_4}(a^3b)$.*

Definition 16.4. *Let X be the set of subgroups $H \subset G$ with action $g \cdot H = gHg^{-1}$. The stabiliser G_H in this case is called the normaliser and denoted*

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

The normaliser $N_G(H)$ is a subgroup that always contains H.

Example 16.6. *We will compute the normaliser of $\langle b \rangle \subset D_3$:*

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

Now $|\langle b \rangle| = 2$ therefore $|N_{D_3}(\langle b \rangle)|$ is 2 or 6. If the normaliser has order 6 then it is the entire group D_3, but $a \notin N_{D_3}(\langle b \rangle)$ as $a\langle b \rangle a^{-1} = \{e, aba^2\} = \{e, a^2b\} \neq \langle b \rangle$. Hence $N_{D_3}(\langle b \rangle) = \langle b \rangle$. This observation is the same as noting that $\langle b \rangle$ is not a normal subgroup of D_3. On the other hand $\langle a \rangle$ is a normal subgroup of D_3 (as it is the kernel of the homomorphism $\phi(a^n b^m) = b^m$) so $N_{D_3}(\langle a \rangle) = D_3$.

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

$$\mathrm{orb}(x) = \{g \cdot x \,|\, \forall\, g \in G\,\}.$$

The orbit of an element $x \in X$ is an equivalence class with the equivalence relation $y \sim x$ if there exists $g \in G$ such that $y = g \cdot x$. This is an equivalence relation as it satisfies:

- (Reflexivity) $x \sim x$ as the identity $e \in G$ always exists satisfying $e \cdot x = x$.
- (Symmetry) $y \sim x \implies x \sim y$ as if $y \sim x$ then $\exists g \in G$ such that $y = g \cdot x$ then $g^{-1} \cdot y = g^{-1} \cdot g \cdot x = x$ therefore $x \sim y$ as $x = g^{-1} \cdot y$ and $g^{-1} \in G$.
- (Transitivity) $x \sim y$ and $y \sim z$ implies that $x = g_1 \cdot y$ and $y = g_2 \cdot z$, hence $x = g_1 \cdot y = g_1 \cdot g_2 \cdot z = (g_1 g_2) \cdot z$, hence $x \sim z$.

As equivalence classes are either disjoint or identical, and every element of X is in some orbit, then the orbits partition X. In particular $|X| = |\mathrm{orb}(x_1)| + |\mathrm{orb}(x_2)| + \ldots + |\mathrm{orb}(x_n)|$ for some choice of representative orbits elements $x_i \in X$.

Example 16.7. *If $X = G$ and $g \cdot x = gx$ then* $\mathrm{orb}(x) = G$ *(while the stabiliser $G_x = \{e\}$).*

Example 16.8. *If X is the set of all subgroups of D_3 with $g \cdot H = gH$ for $H \in X$ then the orbit of $\{e, a, a^2\} = \langle a \rangle$ is*

$$\mathrm{orb}(\langle a \rangle) = \{\langle a \rangle, \{b, ab, a^2 b\}\}.$$

Comment(s).

1. *Let X be the set of all subsets of G with $g \cdot S = gS$, where $S \subset G$ is a subset. Consider $H \subset G$ where H is a subgroup then* $\mathrm{orb}(H)$ *is the set of left cosets of H in G.*
2. *For $X = G$ with $g \cdot x = gxg^{-1}$, then* $\mathrm{orb}(x)$ *is the conjugacy class of x.*

Consider the rotational symmetries of the cube. Each symmetry maps the cube to itself and we may count these symmetries in various ways. We might first argue that at each vertex three faces meet and there are three rotations about the vertex which rotate the faces into each other and a vertex has eight equivalent positions it can occupy on the cube giving $3 \times 8 = 24$ rotational symmetries of the cube. Alternatively, we might consider a face of the cube which has four rotational symmetries and a face can sit in any of six positions on the cube giving $4 \times 6 = 24$ rotational symmetries. There are other ways too. In the first case above the stabiliser of a vertex is isomorphic to $\mathbb{Z}_3$, while the orbit of the vertex has eight elements. In the second counting above, the stabiliser of a face is isomorphic to $\mathbb{Z}_4$ and the orbit of a face has six elements in it. In general we are observing that the stabiliser G_x of an element $s \in X$ (which may be a subset) may be mapped to cosets gG_x which cover the group G: the number of cosets needed to cover G is the number of elements in the orbit of x.

Theorem 16.2. *(The orbit-stabiliser theorem.) Let G be a group and X be a G-set. For each $x \in X$,*

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

Proof. We will show that the number of left cosets of G_x required to cover G is $|\mathrm{orb}(x)|$. We will do this by constructing a bijection between elements of $\mathrm{orb}(x)$ and the cosets gG_x given by

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

Note that this map is injective as suppose there exists $h \in G$ such that $h \cdot x \neq g \cdot x$ such that $M(g \cdot x) = M(h \cdot x)$ then $gG_x = hG_x$ hence $h^{-1}gG_x = G_x$ therefore $h^{-1}g \in G_x$ so $h^{-1} \cdot g \cdot x = x$ implying that $g \cdot x = h \cdot x$. It is surjective by construction, i.e. the pre-image of gG_x is $g \cdot x$. Hence M is a bijection between $g \cdot x$ and the left-coset $gG_x \in \frac{G}{G_x}$. Therefore $|\mathrm{orb}(x)| = \frac{|G|}{|G_x|}$. □

Example 16.9. *Let X be the set of left cosets of the subgroup $H \subset G$ with the G-set action $g \cdot H = gH$. Now $|G_H| = |H|$ and $|\mathrm{orb}(H)| = i(H, G)$, the number of distinct cosets covering G. For this example the orbit-stabiliser theorem gives Lagrange's theorem.*

Example 16.10. *Let $G = D_3 = X$ with action $g \cdot x = gxg^{-1}$. The orbit $\mathrm{orb}(x)$ is the conjugacy class of x. The orbit-stabiliser theorem gives a way to compute the size of the conjugacy classes. For this action the stabiliser G_x is called the centraliser $C_G(x)$. Let us consider the stabilisers of each element of D_3:*

- *When $x = e$, $C_{D_3}(e) = D_3$ then the orbit-stabiliser theorem gives us $|\mathrm{orb}(e)| = \frac{|D_3|}{|C_{D_3}(e)|} = 1$, and $\mathrm{orb}(e) = \{e\}$.*

- *When $x = a$, the centraliser of a contains $\langle a \rangle$ so $|C_{D_3}(a)|$ is 3 or 6, but as D_3 is non-abelian then $C_{D_3}(a) = \langle a \rangle$. Hence by the orbit stabiliser theorem $|\mathrm{orb}(a)| = \frac{|D_3|}{|C_{D_3}(a)|} = 2$, so there are only two elements in the conjugacy class of a, i.e. $\mathrm{orb}(a) = \{a, a^2\}$.*

- *when $x = b$, the centraliser of b contains $\langle b \rangle$ so $|C_{D_3}(b)| = 2$ (as it cannot be 6 because D_3 is non-abelian). Hence, by the orbit-stabiliser theorem $|\mathrm{orb}(b)| = \frac{|D_3|}{|C_{D_3}(b)|} = 3$ and since conjugacy classes cover the group then the conjugacy class of b is $\mathrm{orb}(b) = \{b, ab, a^2b\}$.*

Theorem 16.3. *Let G be a finite group of order p^n where p is prime. 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

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

Now at least one of the conjugacy classes is that of the identity element and so contains just a single element, i.e. $|\mathrm{orb}(e)| = 1$, so

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

As $|G| = p^n$ then the orbit-stabiliser theorem tells us that $|\text{orb(g}_\text{i})| = \frac{|G|}{|C_G(g_i)|} = \frac{p^n}{p^m} = p^{n-m}$, where we have observed that since $C_G(g_i)$ is a sub-group of G then $|C_G(g_i)| = p^m$ for some integer $m \leq n$. We now have:

$$p^n = p^{m_1} + p^{m_2} + \ldots + p^{m_{k-1}} + 1$$

and the left-hand-side of this equation is equal to $0 \mod p$, while the right-hand-side is equal to $1 \mod p$. Therefore at least one more conjugacy class contains only one element. Suppose $|\text{orb}(h)| = 1$ then $ghg^{-1} = h$ for all $g \in G$ implying that $gh = hg$ so $e, h \in Z(G)$ and $|Z(G)| > 1$. □

For example $|D_4| = 8 = 2^3$ and $Z(D_4) = \{e, a^2\}$.

Theorem 16.4. *Let G be a group such that $\frac{G}{Z(G)}$ is a cyclic group. Then G is abelian so $Z(G) = G$.*

Proof. Suppose that $\frac{G}{Z(G)}$ is a cyclic group generated by $gZ(G)$, hence every element of G lies in one of the cosets $g^n Z(G)$ 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

$$g_1 g_2 = g^{n_1} z_1 g^{n_2} z_2 = g^{n_1} g^{n_2} z_1 z_2 = g^{n_1+n_2} z_2 z_1 = g^{n_2} z_2 g^{n_1} z_1 = g_2 g_1.$$

Therefore G is abelian. □

Theorem 16.5. *Any finite group G with $|G| = p^2$ elements, where p is prime, is abelian.*

Proof. As $|G| = p^2$ then $|Z(G)| > 1$. As $Z(G)$ is a sub-group 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 $|\frac{G}{Z(G)}| = p$ is isomorphic to a cyclic group, and this implies $Z(G) = G$ which is a contradiction, so $|Z(G)| = p$ is not allowed. □

We need the following lemma in advance for our next theorem.

Lemma 16.1. *Let G and H be two subgroups of a finite group J. Then*

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

Proof. Note that $G \cap H$ is a subgroup of G and of H and consider $\frac{G}{G \cap H}$. Each element of G is in one of the cosets $g_1(G \cap H), g_2(G \cap H), \ldots g_n(G \cap H)$ with $g_i \neq g_j$ for $i \neq j$ and $g_i^{-1} g_j \notin G \cap H$, so that the cosets are distinct and cover G. Now suppose gh is an element of GH then $gh = g_i g' h$ where $g' \in G \cap H$. As $g', h \in H$ then $gh = g_i(g'h) \in g_i H$. The cosets $g_i H$ are disjoint (as otherwise suppose that $g_iH = g_jH$ then $g_i^{-1}g_j \in H$ and since $g_i, g_j \in G$ then $g_i^{-1}g_j \in G \cap H$ which would contradict our earlier supposition.) Now we know that there are n cosets $g_i(G \cap H)$ covering G, and n cosets g_iH covering GH hence

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

□

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

Proof. The order of each element in G must divide $|G|$, hence each element has order 1, p or p^2. If G has 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 $g \in G$ be a non-identity element of order p, and let $h \in G \setminus \langle g \rangle$ be another element of order p and we note that $\langle g \rangle \cap \langle h \rangle = \{e\}$, as h is in the complement of $\langle g \rangle$. Using our lemma above we see that

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

Hence $\langle g \rangle \langle h \rangle$ covers G and the distinct elements of G take the form $g^n h^m$ for $0 \leq n, m \leq p-1$. Recalling our previous theorem that any group of order p^2 (where p is prime) must be abelian, we can show that $\langle g \rangle \langle h \rangle$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ using $\phi(g^n h^m) = (g^n, h^m) \in \mathbb{Z}_p \times \mathbb{Z}_p$. □

This last theorem is rather neat and means that, up to isomorphism, there are only two distinct groups of each order 4, 9, 25, 49 . . . , both of which are abelian.

17. The Sylow Theorems

Lagrange's theorem states that when H is a subgroup of G then $|H|$ is a factor of $|G|$. The converse statement that if $|H|$ divides $|G|$ then H is a subgroup of G is not always true. For example, the group of even permutations of four objects A_4 has $|A_4| = 12$ but it does not have a subgroup of order 6.[1]

Peter Ludwig Mejdell Sylow (1832-1918) was a Norwegian mathematician who proved a partial converse result: if the divisor is any power of a prime p, i.e. the divisor is of the form p^n for $n \in \mathbb{Z}^+$, then a subgroup always exists. Sylow also showed that if the order of a subgroup is the largest power of a prime that divides the order of a group then all such subgroups are conjugate to each other. For example if $|G| = 60 = 2^2.3.5$ then G contains subgroups of order 3, $4 = 2^2$ and 5, and all subgroups of order 4 are conjugate to each other, as are the subgroups of orders 3 and 5.

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

Comment(s).

1. *The identity element has order 1 which is p^0 for any prime, p.*
2. *Similarly, a p-subgroup is one in which every element is a power of p.*
3. *If G is a p-group then $g_i \in G$ satisfies $g_i^{p^{n_i}} = e$ for $n_i \in \mathbb{Z}^+$, then $|G| = p^k$ for some $k \in \mathbb{Z}^+$.*

Example 17.1. *Any cyclic group of prime order is a p-group.*

[1] Suppose $H \subset A_4$ is a subgroup of order 6 then it is either $\mathbb{Z}_6$ or S_3. Since S_3 contains some odd permutations e.g. (12), (23), (13) then A_4 does not contain S_3 as a subgroup. A_4 contains an element of order 1, three of order 2 and eight of order 3 (which can be checked by constructing A_4 explicitly) hence there is no element of order 6 so A_4 does not have a $\mathbb{Z}_6$ subgroup either.

Example 17.2. *$D_3 = \langle a, b\rangle$ with $a^3 = e$, $b^2 = e$ and $ab = ba^2$ is a group of order $6 = 2.3$ so it is not a p-group but it has a 3-subgroup $\langle a\rangle$ and three 2-subgroups $\{e, b\}$, $\{e, ab\}$ and $\{e, a^2b\}$.*

Definition 17.2. *Let G be a finite group with $|G| = mp^k$ where p is a prime which does not divide $m \in \mathbb{Z}$. A subgroup of order p^k is called a Sylow p-subgroup.*

Example 17.3. *In any group of order $60 = 2^2.3.5$ there are Sylow 2-subgroups (of order 4), Sylow 3-subgroups (of order 3) and Sylow 5-subgroups (of order 5).*

Theorem 17.1. *(The Sylow Theorems.) Let G be a group of order mp^k where p is prime and does not divide m, then:*

I. a Sylow p-subgroup (of order p^k) exists,

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

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

(i) $n_p = 1 \mod p$,

(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 divides m which is the index of the Sylow p-subgroup in G.

Comment(s). *Beware! The numbering and ordering of the Sylow theorems is not universally agreed between mathematicians and texts.*

Lemma 17.1. *The number of ways to pick p^k elements from a set of mp^k elements (where p does not divide m), which is of course equal to $\binom{mp^k}{p^k}$, is $m \mod p$.*

Proof. $\binom{mp^k}{p^k}$ is the coefficient of x^{p^k} in the binomial expansion of $(1+x)^{mp^k} = ((1+x)^{p^k})^m$. Now $(1+x)^{p^k} = \sum_{j=0}^{p^k}\binom{p^k}{j}x^j \cong (1+x^{p^k}) \mod p$. Hence

$$((1+x)^{p^k})^m \cong ((1+x^{p^k}) \mod p)^m = \sum_{j=0}^{m}\binom{m}{j}(x^{p^k})^j \mod p = (1+mx^{p^k}+\ldots) \mod p.$$

Hence the coefficient of x^{p^k} is congruent to $m \mod p$. □

Proof. (Of Sylow I.) Recall that we have a group G such that $|G| = mp^k$. Let S be the set of all subsets of G containing p^k elements. The number of elements (sets) in S is $m \mod p$ by the lemma above. Now let S be a G-set with the action $g \cdot S_i = gS_i = \{gs \,|\, s \in S_i\}$ where S_i is an element of S. The G-set action defines distinct orbits among the elements of S and each orbit may be labelled by a representative set in the orbit, which we will denote $\hat{S}_1$, $\hat{S}_2$,… $\hat{S}_r$.

Note that the number of orbits r is generally distinct from the number of elements of S. The orbits partition S:

$$S = \mathrm{orb}(\hat{S}_1) \cup \mathrm{orb}(\hat{S}_2) \cup \ldots \cup \mathrm{orb}(\hat{S}_r).$$

Our aim will be to show that the stabiliser subgroup of one of these orbits has order p^k. As $|S| = m \mod p$ then at least one of the orbits contains a number of elements which is not divisible by p. Suppose that $\mathrm{orb}(\hat{S}_1)$ is such an orbit and let $|\mathrm{orb}(\hat{S}_1)| = l$, then by the orbit-stabiliser theorem,

$$|G_{\hat{S}_1}| = \frac{|G|}{|\mathrm{orb}(\hat{S}_1)|} = \frac{mp^k}{l} = tp^k$$

for some integer $t = \frac{m}{l}$ (as by construction l is not divisible by p). Now consider $g \in G_{\hat{S}_1}$ then $g \cdot \hat{S}_1 = \hat{S}_1$ so that $gs \in \hat{S}_1$ for all $s \in \hat{S}_1$. Therefore the right-coset $G_{\hat{S}_1}s \subset \hat{S}_1$ and so

$$|G_{\hat{S}_1}| = |G_{\hat{S}_1}s| \leq |\hat{S}_1| = p^k$$

as $\hat{S}_1 \in S$ and so is a set containing p^k elements. As $1 \leq |G_{\hat{S}_1}| \leq p^k$ and also $|G_{\hat{S}_1}| = tp^k$ for $t \in \mathbb{Z}$ then we conclude that $t = 1$ and $|G_{\hat{S}_1}| = p^k$ as required. □

Example 17.4. *In D_3, as $|D_3| = 6 = 2.3$ there are Sylow 2-subgroups (when we take $p = 2$ and $m = 3$) containing two elements and Sylow 3-subgroups (when we take $p = 3$ and $m = 2$) with three elements.*

Example 17.5. $|S_4| = 24 = 2^3.3$, *so S_4 contains a Sylow 3-subgroup containing three elements and a Sylow 2-subgroup containing eight ($= 2^3$) elements.*

Lemma 17.2. *Let P be a Sylow p-subgroup of G, where $|G| = mp^k$. Any p-subgroup of $N_G(P)$ is contained in P and P is the unique Sylow p-subgroup in $N_G(P)$.*

Proof. Let P be a Sylow p-subgroup of G, hence $|P| = p^k$. Evidently $P \subset N_G(P)$ as for any $g \in P$ we have $gPg^{-1} = P$. Let Q be a p-subgroup contained in $N_G(P)$ whose order is p^j, where $j \leq k$. Now $P \lhd N_G(P)$ as, by definition, for $n \in N_G(P)$ we have $nPn^{-1} = P$. In particular if for $x, y \in P$ we have $nxn^{-1} = y$ then $nx = yn$. Now $\langle P, Q \rangle = PQ$ as $Q \subset N_G(P)$ so $qx = yq$ for $q \in Q$ (and one can show that PQ is a group). As $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^{k+j-l}$ where $p^l = |P \cap Q|$. Since P is a Sylow p-subgroup then k is the highest power of p dividing $|G|$ then $l \geq j$. Further as $P \cap Q \subset Q$ then $l \leq j$. Hence $l = j$ and so $P \cap Q = Q$, therefore $Q \subset P$. Now if Q is a Sylow p-subgroup then we must have $j = k$ and hence $Q = P$. Therefore P is the unique Sylow p-subgroup in $N_G(P)$. □

Proof. (Of Sylow II) Let P and Q be two Sylow p-subgroups of a finite group of order mp^k (where p is prime and does not divide m). Our aim is to show that P and Q are conjugate to each other. Consider the collection of sets conjugate to P under the action of G:

$$P_C = \{gPg^{-1} \,|\, g \in G\} = \{P_1, P_2, \ldots, P_r\}$$

N.B. $P_C = \text{orb}(P)$. Under conjugation by elements of P (rather than all of G) P_1, P_2, $\ldots P_r$ are collected into sub-orbits. Let us think about this with the example of D_3 where we take $P = \{e, b\}$, a Sylow 2-subgroup. In this example $P_C = \{\{e, b\}, \{e, a^2b\}, \{e, ab\}\}$ the orbit of P under conjugation by G gives all the Sylow 2-subgroups in D_3. Now under conjugation by elements of $P = \{e, b\}$ we find the sub-orbits:

$$\{e, b\} \xrightarrow{b} \{e, b\}, \quad \{e, a^2b\} \xrightarrow{b} \{e, ab\} \xrightarrow{b} \{e, a^2b\}.$$

We see in the above example that the sub-orbits defined by conjugation with elements of P partition P_C. Returning to the proof for the general case, we will consider the sub-orbits formed by conjugating P_C with elements of P. Evidently $P \in P_C$, let $P_1 = P$ and its orbit under conjugation with P is just P: it is an orbit of length one. We will now argue that there are no other orbits (under conjugation with P) of length one. Suppose, to the contrary, that there exists $P_2 = gPg^{-1}$ whose orbit under P is also of length one, then for $x \in P$ we have $x(gPg^{-1})x^{-1} = gPg^{-1}$ as there is only one element in the P-orbit of P_2 by assumption. Then, $(g^{-1}xg)P(g^{-1}x^{-1}g) = P$ hence $g^{-1}xg \in N_G(P)$. Furthermore each element conjugate to x has order p^k, for some $k \in \mathbb{Z}^+$, therefore $g^{-1}Pg$ is a Sylow p-subgroup in $N_G(P)$. By the previous lemma, such a subgroup is unique hence $g^{-1}Pg = P$ and so $P_2 = gPg^{-1} = P$. Contradicting our assumption that P_2 was a second element of P_C with P-orbit length of one. Now

$$P_C = \text{orb}(P) \cup \text{orb}(\hat{P}_2) \cup \ldots \cup \text{orb}(\hat{P}_s)$$

where P, $\hat{P}_2$, $\ldots \hat{P}_s$ are representatives in the orbits generated by conjugation with P. We note that $|\text{orb}(P)| = 1$ while $|\text{orb}(\hat{P}_i)| > 1$:

$$|P_C| = 1 + |\text{orb}(\hat{P}_2)| + \ldots + |\text{orb}(\hat{P}_s)|.$$

By the orbit-stabiliser theorem $|\text{orb}(\hat{P}_i)| = \frac{|P|}{|N_P(\hat{P}_i)|}$ and as $|P| = p^k$ then each $|\text{orb}(\hat{P}_i)|$ is a power of p greater than zero, i.e. $|\text{orb}(\hat{P}_i)| \mod p = 0$. Therefore $|P_C| = 1 \mod p$. Recall that Q is a second Sylow p-subgroup in G and now consider the orbits of elements of P_C brought about by conjugation with elements of Q. As $Q \subset G$ then this is an automorphism of P_C. The orbits under Q all have length some power of p (as $|Q| = p^k$), and since $|P_C| = 1 \mod p$ then there is one Q-orbit in P_C which is of length one. Suppose that this orbit contains P_2 then for all $w \in Q$ we have $wP_2w^{-1} = w(gPg^{-1})w^{-1} = gPg^{-1}$. As argued earlier, $g^{-1}wg \in N_G(P)$ hence $g^{-1}Qg = P$ and therefore $Q = gPg^{-1}$. Hence all Sylow p-subgroups are conjugate to each other. □

Example 17.6. $|D_5| = 10 = 2.5$, *it has a Sylow* 2*-subgroup* $\langle b\rangle = P$. *Under conjugation of* P *with* D_5 *we find*

$$P_C = \{\{e,b\},\{e,a^2b\},\{e,a^4b\},\{e,ab\},\{e,a^3b\}\}.$$

Now under conjugation with elements of P *these five sets have the* P*-orbits:*

$$\{e,b\} \xrightarrow{b} \{e,b\}, \{e,a^2b\} \overset{b}{\longleftrightarrow} \{e,a^3b\}, \{e,a^4b\} \overset{b}{\longleftrightarrow} \{e,ab\}.$$

So the number of Sylow 2*-subgroups is* $5 = 1+2+2 = 1 \mod 2$. D_5 *also has a Sylow* 5*-subgroup* $\langle a\rangle$, *which we will now take for* P. *Under conjugation of* P *with* D_5 *we find*

$$P_C = \{\{e,a,a^2,a^3,a^4\}\}$$

since $\langle a\rangle \lhd D_5$. *Hence there is just* $1 = 1 \mod 5$ *Sylow* 5 *subgroup.*

Proof. (Of Sylow III).

(i) Consider $P_C = \{gPg^{-1}\,|\,g \in G\}$ we know that $|P_C| = 1 \mod p$ and that each Sylow p-subgroup is contained in P_C. It only remains to show that every gPg^{-1} is a Sylow p-subgroup. But as each gPg^{-1} is a p-group having the same number of elements as P then every set in P_C is a Sylow p-subgroup, therefore $n_p = |P_C| = 1 \mod p$.

(ii) As every Sylow p-subgroup is in the orbit of P under conjugation with elements of G, the orbit-stabiliser theorem tells us that $n_p = |\text{orb}(P)| = \frac{|G|}{|N_G(P)|}$.

(iii) As $P \subset N_G(P)$ then $|N_G(P)| \geq p^k$ and $n_p = \frac{|G|}{|N_G(P)|}$ implies that $|N_G(P)| = \frac{|G|}{n_p} = \frac{m}{n_p}p^k \geq p^k$ where we have used $n_p = 1 \mod p$, so n_p does not divide p^k. Consequently we have n_p divides m.

□

Example 17.7. $|D_3| = 6 = 2.3$

- $n_2 = 1 \mod 2 = 1, 3, 5\ldots$; n_2 *divides* 3 *so* $n_2 = 1$ *or* 3; $n_2 = \frac{6}{|N_{D_3}(P)|}$ *implies that* $|N_{D_3}(P)| = 2$ *or* 6. *Consider the Sylow* 2*-subgroup* $\langle b\rangle$ *then as* $a\langle b\rangle a^{-1} = \{e, aba^{-1}\} = \{e, a^2b\} \neq \langle b\rangle$ *then* $|N_{D_3}(P)| \neq 6$ *so must equal* 2. *Hence* $n_2 = 3$.

- $n_3 = 1 \mod 3 = 1, 4, \ldots$; n_3 *divides* 2 *hence* $n_3 = 1$.

Comment(s). *1. If a Sylow p-subgroup is a normal group then it is the only Sylow p-subgroup as if* $P \lhd G$ *then* $gPg^{-1} = P$ *hence there are no different conjugate groups. Also if there is only one Sylow p-subgroup then it is a normal subgroup as* $n_p = 1$ *implies that* $gPg^{-1} = P$ *for all* $g \in G$. *E.g.* $\langle a\rangle \in D_3$ *is the only Sylow* 3*-subgroup hence it is normal.*

2. *If G is abelian then all subgroups are normal. Hence abelian groups have unique Sylow p-subgroups.*

3. *Sylow subgroups P and Q for different primes p and q can only have a trivial intersection as $P \cap Q$ is a subgroup so its order divides both $|P|$ and $|Q|$ which is only possible if $P \cap Q = \{e\}$.*

Example 17.8. *Any group of order 6 must have a Sylow 2-subgroup, P, and a Sylow 3-subgroup, Q. Now $n_3 = 1, 4, \dots$ and n_3 divides 2 so $n_3 = 1$ therefore $Q \lhd G$. Furthermore $Q \cong \mathbb{Z}_3 = \langle y \rangle$ with $y^3 = e$. Let $P = \langle x \rangle$ with $x^2 = e$. As $Q \lhd G$ then $xyx^{-1} \in Q = \{e, y, y^2\}$. If $xyx^{-1} = e$ then $y = e$ so this case is not possible. Two cases remain:*

(i) *$xyx^{-1} = y$ which implies that $xy = yx$ so that the powers of xy are xy, $(xy)^2 = y^2$, $(xy)^3 = x$, $(xy)^4 = y$, $(xy)^5 = y^2x$, $(xy)^6 = e$. So in this case $G \cong \mathbb{Z}_6$.*

(ii) *$xyx^{-1} = y^2 = y^{-1}$ so that $xy = y^{-1}x$ now $G = \langle x, y \rangle$ with $x^2 = e$, $y^3 = e$ and $xy = y^{-1}x$. Hence $G \cong D_3$.*

Example 17.9. *All groups of order 15 are cyclic. As $|G| = 15 = 3.5$, there are Sylow 3-subgroups and Sylow 5-subgroups. Now $n_3 = 1 \mod 3 = 1, 4, 7, \dots$ and n_3 divides 5 so that $n_3 = 1$; while $n_5 = 1 \mod 5 = 1, 6, 11, \dots$ and n_5 divides 3 therefore $n_5 = 1$. Hence any group of order 15 has a normal Sylow 3-subgroup P and a normal Sylow 5-subgroup Q. Now G has an identity element of order 1, two elements of order 3 in P and four elements of order 5 in Q. This leaves eight other elements. As the order of any element in G is 1, 3, 5 or 15 and there are no more elements of orders 1, 3 or 5 in G, then the remaining eight elements all have order 15. Hence $G \cong \mathbb{Z}_{15} = \langle a \rangle$ which contains $\{e\}$ of order 1, $\{a^5, a^{10}\}$ of order 3, and $\{a^3, a^6, a^9, a^{12}\}$ of order 5.*

18. Tutorial Exercises

TUTORIAL EXERCISES 0

In this tutorial you will work with the definition of a group. The work in this tutorial should be studied during your first tutorial class during the second week of lectures. There is no homework to be submitted for this tutorial.

0.1 Show that the set of all integers forms a group under the multiplication law given by the usual addition of integer numbers. Show that it does not form a group under the multiplication law given by the usual multiplication of integer numbers.

For the next two questions, let e, a, b be three different symbols with the relations $ea = ae = a$, $eb = be = b$, $e^2 = e$, $a^2 = e$, $b^2 = e$ and $aba = bab$.

0.2 Show that set of different words that can be formed from these symbols, taking into account the relations, is $S = \{e, a, b, ab, ba, aba\}$.

0.3 The set S is made into a group by the multiplication law of concatenation of words. To show that the inverse always exist, calculate the inverse of all elements of S in terms of elements of S.

TUTORIAL EXERCISES I

In this tutorial you will work with finite groups of low order. The homework problem should be submitted for feedback during your tutorial.

1.1 Show that the symmetric group S_n is of order n!

1.2 Show that all the matrices of the form

$$\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} ,$$

where μ is any real number, from a group if the law of composition is taken to be matrix multiplication.

1.3 Establish the precise isomorphism between V_4 and $\mathbb{Z}_2 \times \mathbb{Z}_2$ (recall $\mathbb{Z}_2$ is the cyclic group of order 2).

Homework

1.4 Show that the group D_3 generated by the matrices $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $A = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ form a group. Establish the isomorphism with S_3, seen as the set $\{e, a, a^2, b, ab, a^2b\}$ under the relations $a^3 = e, b^2 = e, ab = ba^2$.

TUTORIAL EXERCISES II

In this tutorial you will work with subgroups, the permutation group, equivalence classes, Lagrange's theorem, the dihedral group and direct product groups. The homework problem should be submitted for feedback during your tutorial.

2.1 (a) Show that all the matrices of the form

$$\begin{pmatrix} \lambda & \mu \\ 0 & \lambda \end{pmatrix} ,$$

where λ, μ are real numbers and $\lambda \neq 0$, form a group G if the law of composition is taken to be matrix multiplication.

(b) Show that all the matrices of the form

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} ,$$

where λ is a real number ($\lambda \neq 0$), is a subgroup H of G. Find the right coset space $H\backslash G$.

2.2 The homogeneous modular group $SL(2;\mathbb{Z})$ is

$$SL(2;\mathbb{Z}) = \left\{ \text{all matrices} \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}$$

(a) Verify that $SL(2;\mathbb{Z})$ is a group.

(b) Is $SL(2;\mathbb{Z})$ an abelian group and why?

(c) Is the collection of matrices

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} ,$$

$n \in \mathbb{Z}$, a subgroup of $SL(2,\mathbb{Z})$?

2.3 Show that any group G of order n is isomorphic to a subgroup of the permutation group S_n. CLUE: Associate with every element of the group G a permutation of the elements of G using the group multiplication.

2.4 Let H be a subgroup of G. Then an equivalence relation can be defined on G as follows:

$$a \sim b, \quad \text{if} \quad a^{-1}b \in \mathrm{H}$$

where $a, b \in G$.

(a) Show that $\sim$ is an equivalence relation. (The equivalence classes are called left cosets of G).

(b) Show Lagrange's Theorem for the left cosets.

Homework

2.5 Consider the group D_4 generated by two elements a, b subject to the relations

$$a^4 = b^2 = (ab)^2 = e \ .$$

(a) What is the order of the group?

(b) Give the multiplication table of D_4.

(c) Are the subsets $H_1 = \{a, a^2\}$, $H_2 = \{e, a, a^2, a^3\}$, $H_3 = \{e, b\}$, $H_4 = \{e, ab\}$ and $H_5 = \{a, b\}$ subgroups of G?

(d) Find the right cosets of those subsets above that are subgroups of G and verify Lagrange's theorem.

(e) What are the orders of $D_4 \times D_4$ and $\mathbb{Z}_3 \times D_4$ groups?

TUTORIAL EXERCISES III

The topics covered in this problem set include normal subgroups, homomorphisms, left and right cosets and conjugacy classes. The homework problem should be submitted for feedback during your tutorial.

3.1 Let $\mathbb{C}$ be the complex numbers, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ be the group of non-zero complex numbers with multiplication law the standard complex number multiplication. Let $\mathbb{C}_1$ be the subgroup of $\mathbb{C}^\times$ which is all complex numbers z with absolute value 1, i.e. $|z| = 1$. Show that:

(a) That $\mathbb{C}_1$ is a normal subgroup of $\mathbb{C}^\times$.

(b) That there exists a group homomorphism from $\mathbb{C}^\times$ onto $\mathbb{R}^+$ (the group of positive real numbers with multiplication law the multiplication of real numbers).

(c) That the kernel of this homomorphism is $\mathbb{C}_1$.

(d) That $\mathbb{C}^\times/\mathbb{C}_1$ is isomorphic to $\mathbb{R}^+$.

(e) That $\mathbb{C}^\times$ is isomorphic to $\mathbb{C}_1 \times \mathbb{R}^+$.

3.2 Consider S to be the set of all the transformations $s_{a,b} : \mathbb{R} \to \mathbb{R}$ for all $a \in \mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ and $b \in \mathbb{R}$, where:

$$s_{a,b} : x \mapsto x' = ax + b.$$

(a) Show that S is a group.

(b) Let S_1 be all transformations of the form $x \mapsto x' = x+b$ and S_2 be all transformations of the form $x \mapsto x' = ax$. Show that S_1 and S_2 are subgroups of S.

(c) Show that S_1 is a normal subgroup.

(d) S/S_1 is a group, which group is it (i.e. what group is it isomorphic to)?

Homework

3.3 Consider the group $S_3 = \{e, a, a^2, b, ab, a^2b\}$ with a and b subject to $ba = a^2b,\ ba^2 = ab,\ a^3 = e,\ b^2 = e$. Consider the cyclic subgroup $H = \langle a \rangle = \{e, a, a^2\}$.

(a) Find the right and left cosets of H in S_3 and verify Lagrange's theorem.

(b) Find the conjugacy classes of S_3.

(c) Show that H is a normal subgroup.

(d) What group is $\tilde{G} = S_3/H$ (i.e., again, what standard group is it isomorphic to)? CLUE: Do the latter by finding a suitable homomorphism $\phi : G \to \tilde{G}$ with $\ker(\phi) = H$.

(f) Are the subgroups $\{e, b\}$ and $\{e, ab\}$ normal?

TUTORIAL EXERCISES IV

The topics covered in this problem set include automorphisms, the centre of a group, quotient groups and the homomorphism theorem. The homework problem should be submitted in your tutorial for feedback.

4.1 (a) Let H be a subgroup of a group G. Give the defining property satisfied by H for it to be a normal subgroup of G.

(b) Consider the dihedral group $D_6 =< a, b >$ subject to the relations $a^6 = e$, $b^2 = e$ and $ab = ba^{-1}$, where e is the identity element. Construct the centre of D_6, denoted $Z(D_6)$, and show that it is a normal subgroup of D_6.

(c) Find the left cosets of D_6 with respect to $Z(D_6)$.

An associative multiplication law for subsets S_1 and S_2 of a group G is defined by

$$S_1S_2 = \{s_1s_2 | \forall\, s_1 \in S_1, \forall\, s_2 \in S_2\}.$$

(d) Show that the set $D_6/Z(D_6)$ of left cosets forms a group when the product of two cosets is given by the associative multiplication law for sets defined above. Up to isomorphism, identify the group.

4.2 This question concerns the proof of the homomorphism theorem.

(a) Let G be a group and $H \subset G$ a normal subgroup. We define an associative multiplication law for subsets S_1 and S_2 of G as

$$S_1S_2 = \{s_1s_2 \,|\, s_1 \in S_1, s_2 \in S_2\}.$$

Show that the set of left cosets G/H forms a group under this multiplication law.

(b) Let $\phi : G_1 \to G_2$ be a homomorphism where G_1 and G_2 are both groups. Show that $\ker\phi$ is a normal subgroup of G_1.

(c) Let $\phi : G_1 \to G_2$ be a surjective homomorphism. Show that $G_1/\ker\phi \cong G_2$. Considering the map ψ given by $\psi(g_1H) \equiv \phi(g_1)$ for a suitable normal subgroup H will be useful.

4.3 Let G be a group, $\mathrm{Aut}(G)$ its automorphism group and $\mathrm{Inn}(G)$ the group of inner automorphisms. Show that:

(a) $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

(b) $\mathrm{Inn}(G) \cong G/Z(G)$ where $Z(G)$ is the centre of G. (Clue: Use the map

$$\begin{aligned} \varphi : \quad & G \rightarrow \mathrm{Inn}(G) \\ & g \rightarrow \alpha_g \ , \end{aligned}$$

where $\alpha_g(h) = ghg^{-1}$ for every $h \in G$.)

Homework

4.4 Consider the dihedral group

$$D_4 = \langle a, b \rangle = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

(a) Find the conjugacy classes of D_4.

(b) Find the normal proper subgroups of D_4.

(c) Find the centre $Z(D_4)$.

(d) Find the groups D_4/H where H is a normal proper subgroup of D_4.

(e) Specify the group of inner automorphisms $I(D_4)$ of D_4 (you may use the answer to question 4.3).

TUTORIAL EXERCISES V

The topics covered in this problem set include classical matrix groups, the centre of a group, the dimension of a matrix group and the homomorphism theorem. The homework problem should be submitted in your tutorial for feedback.

5.1 (a) Show that the set

$$GL^+(n;\mathbb{R}) = \{A \in GL(n,\mathbb{R}) : \ \det A > 0\}$$

is a subgroup of $GL(n;\mathbb{R})$.

(b) Show that $GL^+(n;\mathbb{R})$ is a normal subgroup of $GL(n;\mathbb{R})$

(c) Determine the group to which $GL(n;\mathbb{R})/GL^+(n;\mathbb{R})$ is isomorphic.

5.2 Find which group is isomorphic to the quotient group $GL^+(n;\mathbb{R})/Z\big(GL^+(n;\mathbb{R})\big)$ for n odd, where $Z\big(GL^+(n;\mathbb{R})\big)$ is the centre of $GL^+(n;\mathbb{R})$. Note that $Z\big(GL^+(n;\mathbb{R})\big) = \{\lambda\mathbf{1};\lambda \in \mathbb{R}^+\}$. (Hint: find a suitable homomorphism whose kernel is $Z\big(GL^+(n;\mathbb{R})\big)$).

5.3 Using the homomorphism theorem or otherwise, show that

$$GL(N,\mathbb{C})/Z(GL(N,\mathbb{C}) \cong SL(N,\mathbb{C})/Z(SL(N,\mathbb{C})).$$

5.4 The modular group $ML(2;\mathbb{Z})$ is

$$ML(2;\mathbb{Z}) = \left\{\text{all matrices} \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a,b,c,d \in \mathbb{Z} \text{ and } ad-bc \in \{1,-1\}\right\}$$

(a) Show that $ML(2;\mathbb{Z})$ is a group.

(b) Find the centre $Z(ML(2;\mathbb{Z}))$ of this group.

(c) Find the centre of $SL(2;\mathbb{Z}) := \{A \in ML(2;\mathbb{Z}) : \det(A) = 1\}$.

Homework

5.5 Consider the groups $SU(N)$ and $U(N)$.

(a) Show that

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

where $U(1) := \{z \in \mathbb{C} : |z| = 1\}$.

(b) Show that

$$U(N) \cong \big(SU(N) \times U(1)\big)/\mathbb{Z}_N \ .$$

TUTORIAL EXERCISES VI

The topics covered in this problem set include matrix groups and their structure. The homework problem should be submitted in your tutorial for feedback.

6.1 Consider the groups $SO(2)$ and $U(1)$.

(a) Show that $SO(2) \cong U(1)$.

(b) Show that $\mathbb{Z}_2 = \{1, -1\}$ equipped with the standard multiplication is a normal subgroup of $U(1)$.

(c) Find the group $U(1)/\mathbb{Z}_2$ (that is, find which standard group it is isomorphic to).

6.2 Consider the sets M_2 and N_2 given by the matrices

$$M_2 := \left\{ \begin{pmatrix} \lambda^{-1} & 0 \\ \mu & \lambda \end{pmatrix} : \mu, \lambda \in \mathbb{R},\ \lambda \neq 0 \right\}$$

and

$$N_2 := \left\{ \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in \mathbb{R} \right\}$$

respectively.

(a) Show that M_2 and N_2 are groups under matrix multiplication.

(b) Show that N_2 is a normal subgroup of M_2 both directly and by establishing that N_2 is the kernel of a group homomorphism.

(c) Find the coset space M_2/N_2 using the definition of the left cosets of M_2 with respect to N_2.

(d) Find the group M_2/N_2.

6.3 Find the centres of $SU(N),\ N \geq 2$ and $U(N),\ N \geq 2$. What are the groups $SU(N)/Z(SU(N))$ and $U(N)/Z(U(N))$ isomorphic to?

Homework

6.4 (a) State the definition of the matrix group $GL(N, \mathbb{C})$.

(b) Prove that $SL(N, \mathbb{C})$ is a normal subgroup of $GL(N, \mathbb{C})$. Identify the quotient group $GL(N, \mathbb{C})/SL(N, \mathbb{C})$ giving a clear explanation of your answer.

Let a Möbius transformation $f : GL(2, \mathbb{C}) \times \bar{\mathbb{C}} \to \bar{\mathbb{C}}$ where $\bar{\mathbb{C}} = \mathbb{C} \cup \infty$ be given by

$$f(A, z) = \frac{az + b}{cz + d}$$

where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{C})$.

(c) Let $f_A : \bar{\mathbb{C}} \to \bar{\mathbb{C}}$ be given by $f_A(z) = f(A, z)$, so that f_A is a transformation of $\bar{\mathbb{C}}$. Prove that $f_{A_1} \circ f_{A_2} = f_{A_1 A_2}$ for $A_1, A_2 \in GL(2, \mathbb{C})$ where $\circ$ denotes the composition of maps.

(d) Consider the homomorphism $\phi : GL(2, \mathbb{C}) \to \mathrm{Aut}(\bar{\mathbb{C}})$ given by $\phi(A) = f_A$. Compute and identify the kernel of ϕ. Hence prove that

$$\mathrm{Aut}(\bar{\mathbb{C}}) \cong \frac{GL(2, \mathbb{C})}{\ker(\phi)}$$

You may assume that ϕ is a homomorphism whose image is $\mathrm{Aut}(\bar{\mathbb{C}})$.

(e) For $A = \begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix} \in SU(2) \subset GL(2, \mathbb{C})$, show that f_A is a rotation of $\mathbb{C}$. Now by considering the map $\psi : \bar{\mathbb{C}} \to S^2 \subset \mathbb{R}^3$ given by

$$\psi(z) = (\frac{2\mathrm{Re}(z)}{1 + |z|^2}, \frac{2\mathrm{Im}(z)}{1 + |z|^2}, \frac{-1 + |z|^2}{1 + |z|^2})$$

show that f_A induces a rotation R of the sphere S^2 by $R\psi(z) = \psi(f_A(z))$. Identify another element of $SU(2)$ that induces the same rotation R on S^2.

TUTORIAL EXERCISES VII

The topics covered in this problem set include $SU(2)$, the Pauli matrices and the Euclidean group. The homework problem should be submitted for feedback during your tutorial.

7.1 You can use without proof all properties of homomorphisms. Consider, for any $g \in U(1)$, the automorphism $\varphi_g : SU(N) \to SU(N)$ given by $\varphi_g(h) = \omega(g)h\omega(g)^{-1},\ h \in SU(N)$, where $\omega : U(1) \to U(N)$ is the map

$$\omega(z) = \begin{pmatrix} z & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Show that the map $\psi : U(1) \to \mathrm{Aut}(SU(N))$ given by $\psi(g) = \varphi_g$ is a homomorphism (no need to prove that φ_g is an automorphism).

Show that $U(N) \cong U(1) \ltimes_\psi SU(N)$. For this, you may make use of the map Φ acting on $U(N)$ given by

$$\Phi(x) = (\det(x), x\kappa(x)^{-1}), \quad x \in U(N),$$

where $\kappa = \omega \circ \det$. Prove all necessary properties of Φ and κ.

7.2 Show the following:

(a) Without using the Pauli matrices, verify directly that the parameters of $SU(2)$ lie on the three sphere S^3.

(b) Let $U = t + i\boldsymbol{x}.\boldsymbol{\sigma}$, verify that

$$\boldsymbol{y}' \cdot \boldsymbol{\sigma} = U(\boldsymbol{y} \cdot \boldsymbol{\sigma})U^\dagger = (t^2 - \|\boldsymbol{x}\|^2)\boldsymbol{y} \cdot \boldsymbol{\sigma} + 2(\boldsymbol{x}.\boldsymbol{y})\boldsymbol{x} \cdot \boldsymbol{\sigma} - 2t(\boldsymbol{x} \wedge \boldsymbol{y}) \cdot \boldsymbol{\sigma}$$

where $\boldsymbol{x} \wedge \boldsymbol{y}$ denotes the vector-product of $\boldsymbol{x}$ with $\boldsymbol{y}$.

7.3 Find the transformations $\boldsymbol{y} \to \boldsymbol{y}' \equiv R_u\boldsymbol{y}$ induced by $\boldsymbol{y}' \cdot \boldsymbol{\sigma} = U(\boldsymbol{y} \cdot \boldsymbol{\sigma})U^\dagger$ for

(a) $U = \begin{pmatrix} e^{-\frac{i}{2}\alpha} & 0 \\ 0 & e^{\frac{i}{2}\alpha} \end{pmatrix}.$

(b) $U = \begin{pmatrix} \cos\frac{1}{2}\beta & -\sin\frac{1}{2}\beta \\ \sin\frac{1}{2}\beta & \cos\frac{1}{2}\beta \end{pmatrix}.$

Homework

7.4 In this question you will prove that $D_n \cong \mathbb{Z}_2 \ltimes_\psi \mathbb{Z}_n$.

(a) D_n is the group $\langle a, b\rangle$ with $a^n = e$, $b^2 = e$ and $ab = ba^{-1}$. Prove that $\langle a\rangle$ is a normal subgroup of D_n

Let $\psi : \mathbb{Z}_2 \to \text{Aut}(\mathbb{Z}_n)$ be given by $\psi(g) = \phi_g$ where $\phi_g(h) = ghg^{-1}$ for all $g \in \langle b\rangle$ and $h \in \langle a\rangle$.

(b) Show that ϕ_g for each $g \in \langle b\rangle$ is an automorphism of $\mathbb{Z}_n \cong \langle a\rangle$.

(c) Show that ψ is a homomorphism.

Consider the map $\Phi : D_n \to \mathbb{Z}_2 \ltimes_\psi \mathbb{Z}_n$ given by $\Phi(a^p b^q) = (b^q, a^p)$, where $p \in \{0, 1, 2, \ldots n-1\}$ and $q \in \{0, 1\}$.

(d) Show that Φ is an isomorphism.

TUTORIAL EXERCISES VIII

The topics covered in this problem set include the semi-direct product; and the Euclidean group. The homework problem should be submitted in your tutorial for feedback.

8.1 For this question, you can use without proof all basic properties of homomorphisms. Consider, for any $z \in \mathbb{Z}_2 = \{-1, 1\}$, the automorphism $\varphi_z : SO(2) \to SO(2)$ given by $\varphi_z(B) = \omega(z)\, B\, \omega(z)$ for any $B \in SO(2)$, where

$$\omega(z) = \begin{pmatrix} z & 0 \\ 0 & 1 \end{pmatrix}.$$

(a) As stated above, φ_z is an automorphism of $SO(2)$ for each individual z. Now show that the map $\psi : \mathbb{Z}_2 \to \mathrm{Aut}(SO(2))$ given by $\psi(z) = \varphi_z$ is a homomorphism.

(b) Show that $O(2) \cong \mathbb{Z}_2 \ltimes_\psi SO(2)$. For this, you may make use of the map Φ acting on $O(2)$ by

$$\Phi(A) = (\,\det(A)\,,\, A\,\omega(\det(A))\,), \quad A \in O(2).$$

Prove all necessary properties of Φ.

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

(a) Demonstrate explicitly that E_N is a group.

(b) Prove that the group of translations of the Euclidean plane, $\mathbb{R}^N$ is a normal subgroup of E_N.

(c) Construct an isomorphism between the quotient group $\frac{E_N}{\mathbb{R}^N}$ and the orthogonal group $O(N)$.

(d) Compute the real dimension of the Euclidean group E_N.

Homework

8.3 Define the cross product of two vectors V^i and T^i in $\mathbb{R}^3$ as $(V \times T)^i = \sum_{j,k} \epsilon_{ijk} V^j T^k$, where the anti-symmetric symbol ϵ_{ijk} for $i, j, k \in \{1, 2, 3\}$ is defined by

$$\epsilon_{123} = \epsilon_{231} = \epsilon_{312} = 1,$$

$$\epsilon_{321} = \epsilon_{213} = \epsilon_{132} = -1,$$

and all other elements are zero. Consider the transformation

$$\begin{aligned} GL(3,\mathbb{R}) \times \mathbb{R}^3 &\to \mathbb{R}^3 \\ (R, X) &\to RX \end{aligned}$$

Find the conditions on the matrices R such that $(V \times T)$ transforms as a vector under matrix multiplication. For this, use, after you prove it, the identity

$$\sum_{i,j,k} \epsilon_{ijk} A_{im} A_{jn} A_{kp} = \det A \epsilon_{mnp},$$

which is valid for any 3×3 matrix A. Then generalise this to the following case: Consider the transformation

$$\begin{aligned} GL(n,\mathbb{R}) \times \mathbb{R}^n &\to \mathbb{R}^n \\ (R, X) &\to RX \end{aligned}$$

Find the conditions on the matrices R such that

$$Y^i = \sum_{j_1, j_2, \ldots, j_{n-1}} \epsilon_{i j_1 j_2 \ldots j_{n-1}} X_1^{j_1} X_2^{j_2} \ldots X_{n-1}^{j_{n-1}}$$

transforms as a vector under the above transformation, $X_1, \ldots, X_{n-1}$ are vectors in $\mathbb{R}^n$.

TUTORIAL EXERCISES IX

The topics covered in this problem set include the Poincaré group; the Lorentz group; matrix groups; infinitesimal transformations; G-sets, stabilisers and orbits.

9.1 The Poincaré group, P consists of translations and Lorentz rotations in $\mathbb{R}^4$ and so its elements can be denoted by the symbol $(a^\mu, \Lambda^\mu{}_\nu)$ for $a^\mu \ \in \mathbb{R}^4$, $\Lambda^\mu{}_\nu \ \in \ L$ where L is in the Lorentz group (the Lorentz group is the group of 4 by 4 matrices Λ which satisfy $\sum_{\mu,\nu=0}^{3} \eta_{\mu,\nu} \Lambda^\mu{}_\alpha \Lambda^\nu{}_\beta = \eta_{\alpha,\beta}$ where $\eta_{\mu,\nu}$ is -1 if $\mu = \nu = 0$, it is 1 if $\mu = \nu \in \{1,2,3\}$ and it is zero otherwise). Given that the action of such an element of the Poincare group on $x^\mu \ \in \mathbb{R}^4$ is given by

$$x^{\mu\prime} = \sum_\nu \Lambda^\mu{}_\nu x^\nu + a^\mu$$

calculate the composition rule for the Poincare group. Show that all such transformations actually form a group, assuming that the Lorentz group indeed forms a group.

Note

For continuous groups (Lie groups) there is a simple description of the elements that lie near the identity. For this one considers a small number ϵ and writes the elements of G in the neighbourhood of identity e as

$$A = e + \epsilon a \ .$$

Then one can proceed to investigate various properties of the group G working in first order in ϵ. As an example consider the inverse of A. Assuming that A^{-1} is also near the identity, one can write

$$A^{-1} = e + \epsilon b \ .$$

Then the condition

$$A^{-1}A = e$$

implies that

$$(e + \epsilon b)(e + \epsilon a) = e + \epsilon(a + b) + \mathcal{O}(\epsilon^2) = e$$

Thus

$$b = -a \ .$$

Using the above proceed to answer questions [9.2] and [9.3] below.

9.2 Write a matrix R in infinitesimal form i.e. $R = \mathbb{I} + \epsilon r$ and working to lowest order in ϵ show that

(a) R is unitary implies $r^\dagger = -r$.

(b) R is a real orthogonal matrix implies that $r^T = -r$.

(c) $\det R = 1$ implies $\mathrm{Tr}(r) = 0$ (you may assume that R is a diagonalisable matrix, and you may wish to use the formula: $\det R = e^{\mathrm{Tr} \log R}$). Consequently, find a parametrisation of $SO(N)$ and $SU(N)$ in the infinitesimal neighbourhood of the identity element.

9.3 Consider the infinitesimal transformation induced by elements of the type $R = e + \epsilon\Lambda$, $x'_i = x_i + \epsilon \sum_{j=1}^N \Lambda_i{}^j x_j$, and find the conditions on the matrix $\Lambda_i{}^j$ to leave the line element $\|x\|^2 = \sum_{i=1}^N x_i x_i$ invariant, i.e. $\sum_i x'_i x'_i = \sum_i x_i x_i$ to lowest order in ϵ.

9.4 Consider the set of all real polynomials in n variables x_1, x_2, $\ldots x_n$. This set can be equipped with an action for the symmetric group S_n, where the permutation $\pi \in S_n$ permutes the variables as $x_1 \mapsto x_{\pi(1)}$, $x_2 \mapsto x_{\pi(2)}$, $\ldots x_n \mapsto x_{\pi(n)}$. Show that this satisfies the defining properties of a G-set.

9.5 For any G-set X and $x \in X$, prove that the stabiliser G_x is a subgroup of G.

Homework

9.6 Let X be the set of all subsets of G. Construct all the orbits in X generated when

(a) $g \cdot x = gx$ for $x \in X$ when $G = \mathbb{Z}_3$, and

(b) $g \cdot x = gx$ for $x \in X$ when $G = D_3$.

For the final part of the question, let X be the set of all subgroups of G. Construct all the orbits in X generated when

(c) $g \cdot x = gxg^{-1}$ for $x \in X$ when $G = D_3$.

TUTORIAL EXERCISES X

The topics covered in this problem set include G-sets, the orbit-stabiliser theorem, and the Sylow theorems.

10.1 Let $G = GL(N, \mathbb{R})$ and let $X = \mathbb{R}^N$, show that X equipped with the action $M \cdot \boldsymbol{x} = M\boldsymbol{x}$ where $M \in G$ and $\boldsymbol{x} \in X$ is a G-set.

10.2 [1] Let V be a complex vector space with basis $\{v_1, v_2, \ldots v_n\}$ and let $G = S_n$, the symmetric group of all permutations of n elements. For $\pi \in G$ and any $v = \sum_{k=1}^{n} \lambda_k v_k \in V$, define the action

$$\pi \cdot v = \sum_{k=1}^{n} \lambda_k v_{\pi(k)}.$$

Show that V is a G-set, and find both $\mathrm{orb}(v)$ and G_v when

(a) $n = 4$ and $v = v_1 + v_2 + v_3 + v_4$; and

(b) $n = 4$ and $v = v_1 + v_3$.

10.3 Consider the G-set $X = D_{10}$ with action $g \cdot x = gxg^{-1}$. Compute

(a) the centralisers of every element in D_{10}; and

(b) construct all the conjugacy classes of D_{10}.

[Hint: find $Z(D_{10})$ and use the orbit-stabiliser theorem.]

10.4 What do the Sylow theorems allow you to determine about the Sylow 2-subgroups and Sylow 3-subgroups of any group of order 12?

10.5 Let p, q be primes with $p > q$. Prove that any group G of order pq has a normal Sylow p-subgroup. Show that G is either a cyclic group or a semi-direct product group.

Homework

10.6 Prove that every group of order 35 is cyclic.

[1] Question due to John E. Humphreys.