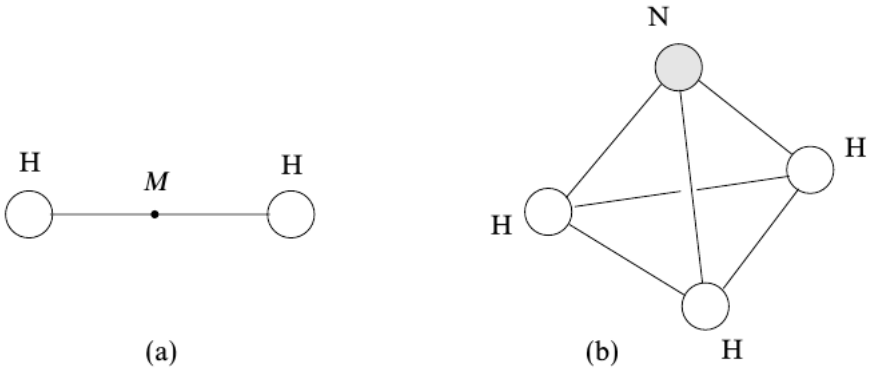
Single Maths A – Easter 2018

Lecture 1

1.1 Groups of symmetries

Groups are algebraic gadgets which are collections of symmetries of some objects. These can be symmetries of some mathematical object, or of a physical object, such as a molecule. Consider this picture of a hydrogen molecule (H_2) and an ammonia molecule (NH_3):



Mathematically, a *symmetry* is a transformation that carries an object into itself. For example, the hydrogen molecule (consisting of two hydrogen atoms) has the following symmetries:

i) Any rotation along its long axis,

ii) Rotation by π about an axis perpendicular to the long axis, and passing through M (which lies midway between the atoms). This symmetry can also be seen as a reflection (mirror image) w.r.t. the plane passing through M, perpendicular to the long axis.

iii) Any combination of the above.

The ammonia molecule is a little bit more complicated. It is a tetrahedron with a nitrogen atom at the top and a base which is an equilateral triangle with hydrogen atoms in the corners. Let A be the axis going through the N-vertex perpendicular to the base triangle. The symmetries of the ammonia molecule are then:

i) Rotations of $2\pi/3$, $4\pi/3$ or 2π about the axis A.

ii) Reflections in each of the three planes containing A and one of the hydrogen atoms.

iii) Any combination of the above.

Remark. If ammonia had another H atom instead of the N at the top, then it would have more symmetries. However, such a molecule doesn't exist in nature.

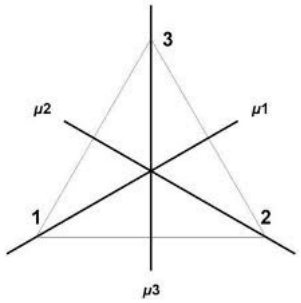
We note three important properties of these collections of symmetries:

- There is an identity symmetry (which brings us back to the initial position, for example rotation by 2π in the ammonia example).
- Composing two symmetries, that is, applying one followed by another, is again a symmetry.
- Every symmetry has an inverse ("do the opposite").

These three properties are the properties that define a *group*. We will give a few more examples, leading up to the precise mathematical definition of group.

1.2 Symmetries of regular n-gons in the plane

Consider an equilateral triangle (aka regular 3-gon):



The vertices are labeled $1, 2, 3$ and there are three reflection axes, μ_1, μ_2, μ_3. The symmetries of the triangle are then:

i) Rotations of $2\pi/3$, $4\pi/3$ or 2π about the centre point of the triangle (compare with the rotation symmetries of the ammonia molecule). Rotating anti-clockwise by $2\pi/3$ has the following effect on the vertices:

$$1 \longrightarrow 2, \qquad 2 \longrightarrow 3, \qquad 3 \longrightarrow 1,$$

that is, the vertices are cycled one step, so the triangle $(1, 2, 3)$ is transformed into $(3, 1, 2)$ (here we denote a triangle by starting from the lower left vertex and going anti-clockwise). Let's call this rotation r.
Rotating by $4\pi/3$ cycles two steps, that is,

$$(1, 2, 3) \longrightarrow (2, 3, 1).$$

This is the same thing as performing the rotation r twice. Viewing the rotation r as a function, the second rotation is $r \circ r = r^2$ (r composed with itself).
Finally, 2π, that is, rotating three steps, brings us back to the initial position, so this rotation is $r \circ r \circ r = r^3 = \mathrm{Id}$, the identity.

ii) Reflecting in the axis μ_1, the triangle $(1,2,3)$ is transformed into $(1,3,2)$; call this transformation s. Applying s twice is the identity, because the mirror image of a mirror image is the original image. Thus $s \circ s = s^2 = \mathrm{Id}$.
Reflecting in μ_2, is $(1,2,3) \longrightarrow (3,2,1)$; call this t.
Reflecting in μ_2, is $(1,2,3) \longrightarrow (2,1,3)$; call this u. As for any reflections, we have $t^2 = u^2 = \mathrm{Id}$.

iii) So far we have six symmetries, three rotations and three reflections:

$$\mathrm{Id}, r, r^2, s, t, u.$$

Are there any more? The only way we could get any more would be by combining a rotation with a reflection, or by combining two reflections (combining two rotations clearly gives another rotation).
If we perform the rotation r followed by the reflection s, we first get the triangle $(3,1,2)$, and then swap the second and third vertices by the reflection s, to get the triangle $(3,2,1)$. This has the same effect as the reflection t. Thus the composition is

$$s \circ r = sr = t.$$

On the other hand, if we first reflect by s and then rotate by r, we first get $(1,3,2)$ and then $(2,1,3)$. Thus

$$r \circ s = rs = u.$$

Thus we can generate the reflections t and u by forming combinations of only r and s.

Next, we check what happens if we combine r^2 with s. The symmetry r^2 gives $(2,3,1)$, and applying s to this gives $(2,1,3)$. Thus

$$sr^2 = u = rs.$$

Taking s first and then r^2 gives $(1,3,2)$, followed by $(3,2,1)$, so

$$r^2 s = t = sr.$$

Moreover, combining the identity with s, r or r^2 does not give anything new, that is,

$$\mathrm{Id}\, r = r\, \mathrm{Id} = r, \qquad \mathrm{Id}\, r^2 = r^2\, \mathrm{Id} = r^2, \qquad \mathrm{Id}\, s = s\, \mathrm{Id} = s.$$

Finally, perhaps the inverse of a symmetry (i.e., doing it backwards) would give something new? The inverse of a rotation (which for us is anti-clockwise) is just a clockwise rotation, and it is clear that going two steps forward (r^2) is the same as one step backwards (r^{-1}), that is,

$$r^{-1} = r^2.$$

Moreover, the inverse $s^{-1} = s$ (because to reverse the effect of s we just apply s again).
We therefore see that we indeed only have six symmetries in total:

$$D_3 = \{\mathrm{Id}, r, r^2, s, rs, r^2 s\}.$$

This is called the *dihedral group* D_3, or the symmetry group of the regular triangle.

Lecture 2

There are several important things to note about this example:

- Composing two symmetries is again a symmetry (we write composition like multiplication).
- Inverting a symmetry is again a symmetry (e.g., inverting r we get r^{-1}, and s is its own inverse).
- In the group D_3, we write composition multiplicatively, but $rs \neq sr$, so composition is an operation which is a bit like multiplication, but does not work the way we are used to.
- We said that D_3 contains *all* symmetries, but you might object that, for example, the product $r^2(r^2s)$ is not in the group. But

  $$r^2(r^2s) = r^3rs = \mathrm{Id}\, rs = rs \in D_3.$$

  Another example is

  $$(rs)(r^2s) = rsr^2s = r(rs)s = r^2s^2 = r^2\,\mathrm{Id} = r^2 \in D_3,$$

  where we have used the relation $sr^2 = rs$ we found above, together with $s^2 = \mathrm{Id}$.
- To describe the group D_3 completely, we only need r and s and three fundamental relations from which everything else follows. We write this as

  $$D_3 = \langle r, s \mid r^3 = \mathrm{Id}, s^2 = \mathrm{Id}, srs = r^2 \rangle.$$

  We say that D_3 is *generated* by r and s. These three relations were determined above.

One can go on and do the same analysis for the symmetries of a square. The group of symmetries here is called the dihedral group D_4. Similarly, for a regular n-gon, for $n \geq 3$, we get the dihedral group D_n. It turns out that

$$D_n = \langle r, s \mid r^n = \mathrm{Id}, s^2 = 1, srs = r^2 \rangle,$$

so the main difference is that in general we have n rotations. It also turns out that D_n consists of $2n$ elements in total, namely

$$D_n = \{\mathrm{Id}, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}.$$

2.1 The definition of group

So, what is a group, mathematically? It is a collection of objects (e.g., symmetries, functions, numbers, matrices, etc) such that we can combine two of them to get a third in the collection, and such that every object has an inverse. More precisely,

Definition 2.1. A set G is called a *group* if the following holds:

i) (Binary operation) For any two elements $x, y \in G$ there is a uniquely defined element $x * y = xy \in G$.

ii) (Associativity) For every three elements $x, y, z \in G$ we have $x(yz) = (xy)z$.

iii) (Identity) There exists an element $\mathrm{Id} \in G$ such that for every $x \in G$ we have $\mathrm{Id} * x = x * \mathrm{Id} = x$.

iv) (Inverses) For every $x \in G$ there is a $x^{-1} \in G$ such that $x * x^{-1} = x^{-1} * x = \mathrm{Id}$.

It is important to understand that the binary operation which we have denoted as multiplication does not have to have anything to do with ordinary multiplication. It can be any binary operation (for D_3 it was composition), such as normal addition. For example, the set of integers

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$$

is a group under the binary operation $+$. Let's check the conditions:

i) For any $a, b \in \mathbb{Z}$, we have $a + b \in \mathbb{Z}$.

ii) For any $a, b, c \in \mathbb{Z}$ we have $a + (b + c) = (a + b) + c$.

iii) We have $\mathrm{Id} = 0$ such that for every $a \in \mathbb{Z}$, $0 + a = a + 0 = a$.

iv) For every $a \in \mathbb{Z}$ we have $-a \in \mathbb{Z}$ such that $a + (-a) = (-a) + a = 0$.

So here $* = +$ and $\mathrm{Id} = 0$.

Note that the set of integers $\mathbb{Z}$ is not a group under normal multiplication, because if $* = \times$, then $\mathrm{Id} = 1$ and $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$, so the fourth condition fails.

We will now give several further examples of groups:

Example 2.2.

i) The set of rational numbers

$$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$$

is a group under addition with $\mathrm{Id} = 0$. The subset

$$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\},$$

($\mathbb{Q}$ with the zero removed) is a group under multiplication, with $\mathrm{Id} = 1$ (we had to remove zero because it does not have a multiplicative inverse). Ditto for $\mathbb{Q}$ replaced by the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$.

ii) A vector space V is a group under addition (see Lecture 18 from last term) (but it also has scalar multiplication, which is not relevant for its group structure).

iii) The set of invertible matrices

$$\mathrm{GL}_n(\mathbb{C}) = \{A \in \mathrm{M}_n(\mathbb{C}) \mid \det A \neq 0\}$$

is called the *general linear group* over $\mathbb{C}$ (it could be over $\mathbb{Q}$ or $\mathbb{R}$ as well). It is a group under matrix multiplication with $\mathrm{Id} = I_n$, the identity matrix. The only thing to check is: 1) that if A and B have inverses, then so do AB (this is true because the inverse of AB is $B^{-1}A^{-1}$) and 2) that $A(BC) = (AB)C$ (which we take for granted here).

Lecture 3

iv) The *circle group*

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\} = \{e^{i\theta} \mid 0 \leq \theta \leq 2\pi\}.$$

Elements in S^1 can be thought of as rotations in the plane by an angle θ, centred at the origin.

v) The symmetry group of the hydrogen molecule mentioned earlier is generated by the circular rotations in S^1 together with one reflections, which we can call s.

vi) The symmetry group of ammonia is in fact just D_3, because its 3D-symmetries can be identified with the 2D-symmetries of the triangle.

Definition 3.1. A group G is said to be *abelian* if $xy = yx$, for all $x, y \in G$.

For example, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}^\times$ and any vector space V are abelian groups. But D_n is not abelian when $n \geq 3$ and $\mathrm{GL}_n(\mathbb{C})$ is not abelian when $n \geq 2$.

To understand groups well, we also need to see some non-examples:

Example 3.2.

i) The natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$ do not form a group under addition because even though the first three conditions in Definition 2.1 hold, the fourth one fails: $-1 \notin \mathbb{N}$. Under multiplication, the fourth condition also fails.

ii) Consider $\mathbb{Z}$ with the binary operation given by subtraction

$$x * y = x - y,$$

so e.g., $2 * 3 = 2 - 3 = -1$, and condition 1 for a group holds. However, we don't have associativity, because

$$2 * (3 * 5) = 2 - (3 - 5) = 4 \neq (2 * 3) * 5 = -6.$$

Neither do we have an identity, because even though

$$x * 0 = x - 0 = x,$$

for all $x \in \mathbb{Z}$, we have $0 * 1 = -1 \neq 1$. So conditions 2,3 and 4 fail.

3.1 Finite cyclic groups

If $n \geq 2$ is an integer, and a is some integer, we write $a \mod n$ for the remainder of a after division by n. For example, if $n = 3$ and $a = 17$, then the remainder is $17 \mod 3 = 2$. If a is divisible by 3, then $a \mod 3 = 0$.

Let

$$\mathbb{Z}/n = \{0, 1, 2, \dots, n-1\}$$

with the binary operation

$$a * b = (a + b) \mod n.$$

Then, $\mathbb{Z}/n$ is a group, because:

i) Binary operation: $*$

ii) Associativity: $a * (b * c) = (a + (b + c)) \mod n = ((a + b) + c) \mod n = (a * b) * c$.

iii) $\mathrm{Id} = 0$.

iv) The inverse a^{-1} is $n - a \mod n$: $a + (n - a) \mod n = (n - a) + a \mod n = 0$.

The groups $\mathbb{Z}/n$ are called the finite *cyclic* groups. The name cyclic comes from the fact that each is generated by a single element 1: For example,

$$\mathbb{Z}/3 = \{1, 1 + 1, 1 + 1 + 1 \mod 3 = 0\},$$

and when we reach n, we "cycle back" to the beginning.

The finite cyclic groups are abelian, because $a * b = (a + b) \mod n = (b + a) \mod n = b * a$.

3.2 Subgroups

Definition 3.3. If G is a group and $H \subseteq G$ as subset, then H is called a subgroup of G if H is itself a group under the same operation as in G.

Example 3.4.

- $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ under addition.
- The set
$$\mathrm{SL}_n(\mathbb{C}) = \{A \in \mathrm{M}_n(\mathbb{C}) \mid \det A = 1\}$$
is a subgroup of $\mathrm{GL}_n(\mathbb{C})$: If A and B are matrices with determinant 1, then
$$\det(AB) = \det(A)\det(B) = 1,$$
so the product AB is also in $\mathrm{SL}_n(\mathbb{C})$.
- The subset $\{\mathrm{Id}, r, r^2\} \subset D_3$ consisting of only rotations, is a subgroup. Similarly, $\{\mathrm{Id}, s\} \subset D_3$ consisting of only reflections, is a subgroup.

Lecture 4

4.1 Maps between groups

Sometimes we can identify two groups as being essentially the same, but written in different ways. To make a connection between two groups, we need a function, or map, between them.

For example, the subgroup $\{\mathrm{Id}, r, r^2\} \subset D_3$ of rotations is essentially the same as the cyclic group $\mathbb{Z}/3$. Indeed, we have a map between them

$$\begin{aligned} \mathrm{Id} &\longmapsto 0, \\ r &\longmapsto 1, \\ r^2 &\longmapsto 2. \end{aligned}$$

This is a function $\varphi : \{\mathrm{Id}, r, r^2\} \to \mathbb{Z}/3$, which is clearly a bijection (i.e., one-to-one). But φ also has another important property, namely that the operation in $\{\mathrm{Id}, r, r^2\}$ (i.e., composition of rotations) is carried into the operation in $\mathbb{Z}/3$ (namely, addition mod 3). To check this, we write

$$\varphi(r \cdot r^2) = \varphi(\mathrm{Id}) = 0 = 1 + 2 \mod 3 = \varphi(r) + \varphi(r^2) \mod 3.$$

We should also check all the other possible products $\varphi(\mathrm{Id}\, r)$ and $\varphi(\mathrm{Id}\, r^2)$, but these are very simple because Id does not change the elements.

It is the bijection φ which carries one operation to the other, which makes these two groups have the same structure, and so be essentially the same. This is formulated in the following definition:

Definition 4.1. If G is a group with operation $*_G$ and H another group with operation $*_H$ then we say that G and H are *isomorphic* if there exists a bijection $\varphi : G \to H$ such that

$$\varphi(x *_G y) = \varphi(x) *_H \varphi(y),$$

for all $x, y \in G$.

We finish by giving another example of this:

Example 4.2. Let $G = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \mid 0 \le \theta < 2\pi \right\}$. We claim that G is a subgroup of $\mathrm{GL}_n(\mathbb{C})$ and that it is isomorphic to the circle group S^1. Indeed, multiplying two such matrices

$$\begin{aligned} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\sigma & \sin\sigma \\ -\sin\sigma & \cos\sigma \end{pmatrix} &= \begin{pmatrix} \cos\theta\cos\sigma - \sin\theta\sin\sigma & \cos\theta\sin\sigma + \sin\theta\cos\sigma \\ -\sin\theta\cos\sigma - \cos\theta\sin\sigma & -\sin\theta\sin\sigma + \cos\theta\cos\sigma \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta+\sigma) & \sin(\theta+\sigma) \\ -\sin(\theta+\sigma) & \cos(\theta+\sigma) \end{pmatrix} \in G. \end{aligned}$$

This also makes it clear that

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

so every element in G has an inverse in G. This is enough to make G a subgroup.

Now, consider the map

$$\varphi : G \longrightarrow S^1 = \{e^{i\theta} \mid 0 \leq \theta < 2\pi\}$$
$$\varphi \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = e^{i\theta}.$$

This is a bijection because it is clearly one-to-one. Finally, we have

$$\varphi \left(\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\sigma & \sin\sigma \\ -\sin\sigma & \cos\sigma \end{pmatrix} \right) = \varphi \begin{pmatrix} \cos(\theta+\sigma) & \sin(\theta+\sigma) \\ -\sin(\theta+\sigma) & \cos(\theta+\sigma) \end{pmatrix} = e^{i(\theta+\sigma)}$$
$$= e^{i\theta} e^{i\sigma} = \varphi \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \varphi \begin{pmatrix} \cos\sigma & \sin\sigma \\ -\sin\sigma & \cos\sigma \end{pmatrix}.$$

Thus φ is an isomorphism, and G is just another way of writing the circle group.