Group Theory (MA343): Lecture Notes
Semester I 2013-2014

Dr Rachel Quinlan
School of Mathematics, Statistics and Applied Mathematics, NUI Galway

November 21, 2013

Contents

Chapter 1

What is a group?

1.1 Examples

This section contains a list of *algebraic structures* with different properties. Although these objects looks different from each other, they do have some features in common, for example they are all equipped with algebraic operations (like addition, multiplication etc.). The properties of these operations can be studied and compared. An important theme of group theory (and all areas of abstract algebra) is the distinction between *essential* and *superficial* similarities and differences in algebraic structures.

1. $(\mathbb{Z}, +)$
   $\mathbb{Z}$ is the set of integers, $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
   The "$+$" indicates that we are thinking of $\mathbb{Z}$ as being equipped with addition. This means that given any pair of integers a and b we can produce a new integer by taking their sum $a + b$.

2. $(\mathbb{C}^\times, \times)$
   Here $\mathbb{C}^\times$ denotes the set of *non-zero* complex numbers, and "$\times$" denotes multiplication of complex numbers. So for example

   $$(2 + 3i) \times (1 - i) = 5 + i.$$

   The product of two elements of $\mathbb{C}^\times$ is always an element of $\mathbb{C}^\times$ (we say that $C^\times$ is *closed* under multiplication of complex numbers). So "$\times$" is a *binary operation* on $\mathbb{C}^\times$.

3. $(\mathrm{GL}(2, \mathbb{Q}), \times)$
   Read this as "the general linear group of 2 by 2 matrices over the rational numbers" ("GL" stands for "general linear").

   $$\mathrm{GL}(2, \mathbb{Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Q}; ad - bc \neq 0 \right\},$$

   so we are talking about the set of 2 by 2 matrices that have rational entries and have non-zero determinant or equivalently that have inverses. The "$\times$" here stands for matrix multiplication. Note that if A and B are elements of $\mathrm{GL}(2, \mathbb{Q})$, then so also is $A \times B$ (and $B \times A$ which might be different).
   Question: Is this obvious? Why is it true?

4. $(\{1, i, -i, -1\}, \times)$
   Here we are talking about the set of complex fourth roots of unity, under multiplication of complex numbers. Note that this set is closed under multiplication, meaning that the product of any two elements of the set is again in the set. You can check this directly by writing out the whole multiplication table (a worthwhile exercise at this point).

5. Let S_4 denote the set of all permutations of the set $\{a, b, c, d\}$.
Recall that a *permutation* of the set $\{a, b, c, d\}$ is a bijective function from the set to itself. The permutation

$$\begin{aligned} a &\longrightarrow d \\ b &\longrightarrow b \\ c &\longrightarrow a \\ d &\longrightarrow c \end{aligned}$$

is sometimes written as $\begin{pmatrix} a & b & c & d \\ d & b & a & c \end{pmatrix}$.

Given two permutations σ and τ of $\{a, b, c, d\}$, we can *compose* them to form the functions $\sigma \circ \tau$ (σ after τ) and $\tau \circ \sigma$ (τ after σ). This composition works as for any functions and is often referred to as *multiplication* of permutations.

Claim: The functions $\sigma \circ \tau$ and $\tau \circ \sigma$ are again *permutations* of $\{a, b, c, d\}$.
Why is this true? Can you prove it as an exercise?

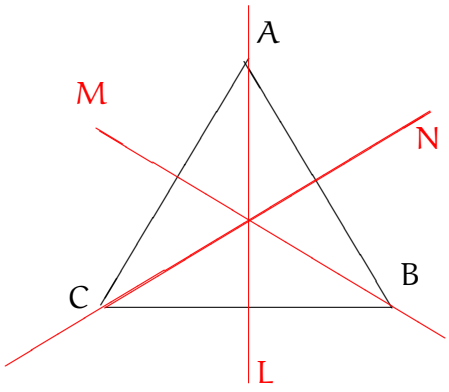
Question: Would you expect $\sigma \circ \tau$ and $\tau \circ \sigma$ to be the same function? If in doubt, try some examples.

Note: It is a good idea to recall/revise what you know about multiplication of permutations and the expression of permutations as products of disjoint cycles and products of transpositions, this topic will be important in this course.

6. **General groups of symmetries**
Suppose that P is some connected object in the two-dimensional plane, like a polygon or a line segment or a curve or a disc (*connected* means all in one piece). The following is an informal (and temporary) description of what is meant by a *symmetry* of P. Imagine that P is an object made of a rigid material. If you can pick up this piece of material from the plane and move it around (in 3-dimensional space) without breaking, compressing, stretching or deforming it in any way, and put it back so that the object occupies the same space that it originally did, you have implemented a symmetry of P.

For example, if P is a circular disc, then symmetries of P include rotations about the centre through any angle, reflections in any diameter, and any composition of operations of these kinds. Two symmetries are considered to be the same if P ends up in exactly the same position after both of them - for example in the case of the circular disc, a counter-clockwise rotation about the centre through a full 360° is the same as the rotation through 0° or the rotation through 720°.

7. **Symmetries of an equilateral triangle**
Consider an equilateral triangle with vertices labelled A, B, C as in the diagram. For this example it does not matter whether you think of the triangle as consisting just of the vertices and edges or as a triangular disc.



The triangle has six symmetries:

- the identity symmetry I, which leaves everything where it is
- the counterclockwise rotation R_{120} through 120° about the centroid
- the counterclockwise rotation R_{240} through 240° about the centroid
- the reflections in the three medians: call these S_L, S_M, S_N.

Let D_6 denote the set of these six symmetries.
Note that the first three (the rotations) preserve the order in which the vertices A, B, C are encountered as you travel around the perimeter in a counter-clockwise direction; the last three (the reflections) change this order. If you think of the object as a "filled-in" disc, the reflections involve flipping it over and the rotations don't.

Now that we have these six symmetries, we can compose pairs of them together. *Example*: We define $R_{120} \circ S_L$ (read the "$\circ$" as "after") to be the symmetry that first reflects the triangle in the vertical line L and then applies the counter-clockwise rotation through 120°. The overall effect of this leaves vertex B fixed and interchanges the other two, so it is the same as S_M - convince yourself of this, using a physical triangle if necessary. For every pair of our six symmetries, we can figure out what their composition is and write out the whole composition table, which is partly completed below. The entry in this table in the position whose row is labelled with the symmetry τ and whose column is labelled with the symmetry σ is $\tau \circ \sigma$.

$(D_6, \circ)$	I	R_{120}	R_{240}	S_L	S_M	S_N
I	I	R_{120}	R_{240}	S_L	S_M	S_N
R_{120}	R_{120}	R_{240}	I	S_M	S_N	S_L
R_{240}						
S_L	S_L	S_N	S_M	I	R_{240}	R_{120}
S_M						
S_N						

Important Exercise: By thinking about the compositions of all these symmetries, verify the part of the above table that is filled in and fill in the rest of it. You should find that each element of D_6 *appears exactly once in each row and in each column.*

One way to think about symmetries of the triangle is as geometric operations as above. Another is as permutations of the vertices. For example the reflection in the line L fixes the vertex A and swaps the other two, it corresponds to the permutation

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}.$$

The rotation R_{120} moves vertex A to the position of C, C to the position of B, and B to the position of A. It corresponds to the permutation

$$\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}.$$

Another Important Exercise: Write down the permutations corresponding to the remaining elements of D_6 *and verify that with this interpretation the composition of symmetries as defined above and the multiplication of permutations really amount to the same thing in this context (this means confirming that the permutation corresponding to the composition of two symmetries of the triangle is what you would expect based on the product of the two corresponding permutations).*

Does *every* permutation of the vertices of the triangle arise from a symmetry? If so, what the second important exercise is really saying is that the set of symmetries of an equilateral triangle (with composition) is essentially the same object as the set of permutations of the set $\{A, B, C\}$, with permutation multiplication.

Part of our work in this course will be to precisely formulate what is meant by "essentially the same" here and to develop the conceptual tools and language to discuss situations like this. The examples in this section will hopefully be useful as our account of the subject becomes more technical and abstract.

8. Symmetries of a square
   Consider a square with vertices labelled A, B, C, D (in cyclic order as you travel around the perimeter). Let D_8 denote the set of symmetries of the square.
   Exercise: How many elements does D_8 *have? Describe them in terms of rotations and reflections. Write down the permutation of* $\{A, B, C, D\}$ *corresponding to each one. Does every permutation of this set arise from a symmetry of the square?*

1.2 The axioms of a group

It's time now to see the formal definition of a group. After this you should carefully check that each of the examples in Section 1.1 *is* indeed a group, and identify in each case the identity element and the inverse of a typical element. The formal definition is stated below followed by some explanatory notes.

Definition 1.2.1. *A* group G *is a non-empty set equipped with a binary operation* $\star$*, in which the following axioms hold.*

1. $\star$ *is an* associative operation. *This means that for any elements* x, y, z *of* G

$$(x \star y) \star z = x \star (y \star z).$$

2. *Some element* id *of* G *is an* identity element *for* $\star$. *This means that for every element* x *of* G

$$\mathrm{id} \star x = x \star \mathrm{id} = x.$$

3. *For every element* x *of* G *there is an element* x^{-1} *of* G *that is an* inverse *of* G *with respect to* $\star$.

Notes

1. *The first line of the definition*
   A binary operation on a set G is a way of combining two elements of G (in specified order) to produce a new element of G. Technically it is a function from G $\times$ G (the set of ordered pairs of elements of G) to G. For example:

   - Addition is a binary operation on the set $\mathbb{N}$ of natural numbers.
   - Subtraction is *not* a binary operation on $\mathbb{N}$. *Why not*?
   - Matrix multiplication is a binary operation on the set $M_3(\mathbb{Q})$ of 3×3 matrices with rational entries (but not on the set of *all* square matrices with rational entries - why?).

   Implicit in the statement that $\star$ is a binary operation on G is the condition that when you use $\star$ to combine two elements of G, the result is again an element of G, i.e. that G is *closed* under $\star$. Some authors list this as one of the axioms of a group - you may see this in some books.

2. *Associativity* is a property that some operations have and that some do not. Our first axiom says that in order for a structure to be considered a group, its binary operation must be associative. People do consider algebraic structures that have non-associative operations, the most commonly encountered examples are *Lie Algebras*.
   Exercise: Give an example of a familiar binary operation (on $\mathbb{Z}$ for example) that is not associative.

3. An identity element for a binary operation is sometimes referred to as a *neutral element*, a term which is probably more self-explanatory although less prominent. An identity element for a binary operation $\star$ is one that has no effect on any element when combined with that element using $\star$. For example, 0 is an identity element for addition in $\mathbb{Z}$, 1 is an identity element for multiplication in $\mathbb{Z}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is an identity element for multiplication of 2×2 matrices.
   Important exercise: In each of the examples in Section 1.1, identify the identity element.

4. If we have an identity element for some binary operation, we can consider whether certain elements have *inverses* or not. Two elements x and y are *inverses* of each other with respect to the binary operation $\star$ if $x \star y$ and $y \star x$ are both equal to the identity element. For example, -5 and 5 are inverses for each other in $\mathbb{Z}$; this means that adding -5 to some

integer "reverses" the work of adding 5. The rational numbers $\frac{2}{5}$ and $\frac{5}{2}$ are inverses of each other for multipication in $\mathbb{Q}$; this means we can "undo" the work of multiplying by $\frac{5}{2}$ if we multiply by 25. Of course we could describe these examples in terms of subtracting and dividing, but it is helpful to get used to thinking in terms of inverses if you can, we will not always have notions of subtraction and division. It is entirely possible for an element to be its own inverse - this is the case for the identity element of every group, and also for example for the reflections in D_6 or for the element $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ of $GL(2, \mathbb{Q})$.

Important exercise: In each of the examples in Section 1.1, identify the inverse of a typical element.

Note: In order to talk about inverses, you must have a particular binary operation in mind and your set must have an identity element for that operation.

Definition 1.2.1 is the criterion that decides whether a given algebraic structure is a group or not.

Problem 1.2.2. *Let* $UT_3(\mathbb{Q})$ *be the set of* 3×3 *upper triangular matrices with rational entries. Is* $UT_3(\mathbb{Q})$ *a group under matrix multiplication?*

Recall that a square matrix A is *upper triangular* if all entries below its main diagonal are zeros (or equivalently if $A_{ij} = 0$ whenever $i > j$). To answer this question you must ask yourself:

- Is $UT_3(\mathbb{Q})$ closed under matrix multiplication?
- Is the operation associative? (In most examples of interest the answer is yes as in this case - multiplication of $n \times n$ matrices is always associative).
- Does this set contain an identity element for the operation? (In this example this question amounts to whether the identity element for multiplication of 3×3 matrices is upper triangular).
- Does every element of the set have an inverse that belongs to the set?

To confirm that your object is a group, you need to check that all of these questions have a positive answer. If you find that one of them has a negative answer, that is enough to justify the conclusion that your object is not a group. The answer is no in the case of Problem 1.2.2. Why?

Problem 1.2.3. *Let* S *be the set of* 3×3 *upper triangular matrices with rational entries, in which no element has a zero entry on the main diagonal. Is* S *a group under matrix multiplication?*

We conclude this section by mentioning two obvious and important dichotomies in group theory. Definition 1.2.1 says that a group must be a non-empty set but says nothing about how many elements it can have. A group is called *infinite* if it has infinitely many elements and *finite* if it has finitely many elements. The study of infinite groups tends to have quite a different flavour from the study of finite groups, essentially because in the later case we can do things like count elements (in the whole group or in a subset of interest).
Exercise Determine which of the examples in Section 1.1 are finite.

Recall that a binary operation $\star$ on a set S is *commutative* if

$$x \star y = y \star x$$

for all elements x, y of S. There is nothing in Definition 1.2.1 requiring that a group operation be commutative. A group whose operation *is* commutative is called *abelian*, after the Norwegian mathematician Niels Henrik Abel (1802–1829).
Exercise Determine which of the examples in Section 1.1 are abelian.
For example, the multiplicative group $\mathbb{C}^\times$ (or$(\mathbb{C}^\times, \times)$) of the complex numbers is abelian, but $GL(2, Q)$ is not.

Remark on Notation: Especially in the non-abelian case, the identity element of a group is often referred to as 1 (whether it is the *number* 1 or not) and the result of combining the elements a and b with the group operation is often just written ab - i.e. there is no particular symbol like $\times$ or $\circ$ or whatever used within the product. This is just a notational convention and worth getting used to - it makes writing simpler when you do get used to it.

Abelian groups are often written with the operation referred to as *addition* and denoted $+$, and the identity element denoted as 0. This makes sense of course if the operation naturally is a version of addition (of numbers, matrices or functions for example), but sometimes the additive notation is also used in an abstract context. The symbol "$+$" would never conventionally be used for a non-commutative operation.

Remark on History: The modern definition of a group (Definition 1.2.1) is nowadays a starting point for the study of group theory. It was not the starting point in the development of the subject although it was a significant milestone. The first abstract definition of a group was given by Arthur Cayley in 1854. This arose from several decades of work on what are now called groups of permutations and on solving polynonial equations by Lagrange, Abel and Galois among others, and on groups of symmetries in geometry by Klein. The introduction of an abstract definition brought the subject into its modern form and had a massive impact on the development of algebra.

1.3 Subgroups and generating sets

A common approach to understanding algebraic structures is to try to find smaller structures within them that have similar properties. In the case of groups such things are called subgroups.

Example 1.3.1. ***The special linear groups***
Recall that $\mathrm{GL}(3,\mathbb{Q})$*, the set of* 3×3 *matrices that have rational entries and have non-zero determinant, is a group under matrix multiplication. Within this let* $\mathrm{SL}(3,\mathbb{Q})$ *denote the set of elements whose determinant is* 1*. Then*

1. $\mathrm{SL}(3,\mathbb{Q})$ *is closed under matrix multiplication.*
   What is required to show this is that whenever A *and* B *belong to* $\mathrm{SL}(3,\mathbb{Q})$*, then so does their product* AB*. To confirm that this is true we need to look at the defining properties of elements of* $\mathrm{SL}(3,\mathbb{Q})$ *and at how they behave under matrix multiplication.*

   So let $A, B \in \mathrm{SL}(3,\mathbb{Q})$.
   This means that A *and* B *are* 3×3 *rational matrices and* $\det(A) = \det(B) = 1$.
   Then $\det(AB) = \det(A)\det(B) = 1\times 1 = 1$.
   So $AB \in \mathrm{SL}(3,\mathbb{Q})$ *also.*
   (Note that this relies on the multiplicative property of the determinant)

2. *The identity matrix belongs to* $\mathrm{SL}(3,\mathbb{Q})$ *(since its determinant is 1).*

3. *Suppose that* A *belongs to* $\mathrm{SL}(3,\mathbb{Q})$*. Then so also does* A^{-1}*, since*

$$\det A^{-1} = \frac{1}{\det A} = \frac{1}{1} = 1.$$

It follows that $\mathrm{SL}(3,\mathbb{Q})$ *is itself a group under matrix multiplication. We say that it is a* subgroup *of* $\mathrm{GL}(3,\mathbb{Q})$.

Terminology: $\mathrm{SL}(3,\mathbb{Q})$ is called the *special linear group* of 3×3 matrices over $\mathbb{Q}$ with determinant 1. The general linear group includes all invertible matrices; the special linear group only includes those with determinant 1.

Definition 1.3.2. *Let* G *be a group and let* H *be a subset of* G*. Then* H *is called a* subgroup *of* G *if* H *is itself a group under the operation of* G.

Every group has a *trivial subgroup* consisting only of the identity element, and every group is a subgroup of itself. A *proper subgroup* is one that is not equal to the whole group.
Not every group has non-trivial proper subgroups. For example, let $\zeta = e^{2\pi i/5}$. Then $\zeta^5 = 1 \in \mathbb{C}$, so ζ is a complex 5th root of unity. The full set of complex fifth roots of unity is

$$\{1, e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}, e^{8\pi i/5}\} = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4\}.$$

These five numbers form a group G_5 under multiplication of complex numbers (note that they occur at the vertices of a regular pentagon in the Argand plane). The full group table is below.

$G_5, \times$	1	ζ	ζ^2	ζ^3	ζ^4
1	1	ζ	ζ^2	ζ^3	ζ^4
ζ	ζ	ζ^2	ζ^3	ζ^4	1
ζ^2	ζ^2	ζ^3	ζ^4	1	ζ
ζ^3	ζ^3	ζ^4	1	ζ	ζ^2
ζ^4	ζ^4	1	ζ	ζ^2	ζ^3

Claim: G_5 has no non-trivial proper subgroup.
To see this, take the element ζ. Suppose that H is a subgroup of G_5 that contains ζ. What else must H contain? Can you show that H must include all of the elements of G_5? Repeat this for each of the other non-zero elements of G_5.

So it is not automatic that a group will have non-trivial proper subgroups. Nevertheless they often do, as in the following examples/exercises.

1. Let D_{2n} be the *dihedral group* consisting of the symmetries of a regular polygon with n sides. So D_{2n} consists of n rotational symmetries and n reflections. The set of rotational symmetries is a subgroup with n elements. To verify this means verifying that

   - The composition of two rotations is a rotation.
   - The inverse of a rotation is a rotation.

   Is the set of reflections in D_{2n} a subgroup? Why or why not?

2. Let S_5 be the group of permutations of the set $\{a, b, c, d, e\}$.
   How many elements are in S_5?
   Let H_1 be the subset of S_5 consisting of those elements that fix a (and permute b, c, d, e). Show that H_1 is a subgroup of S_5. How many elements are in H_1?
   Let H_2 be the subset of S_5 consisting of those elements that fix the set $\{a, b\}$ (this includes those elements that fix both a and b and those that swap a and b). Show that H_2 is a subgroup of S_5. How many elements are in H_2?
   Let H_3 denote the intersection of H_1 and H_2. How many elements does it have? Is it a subgroup of S_5?

3. Let $\mathbb{C}^\times$ denote the group of non-zero complex numbers, under multiplication. The following are some examples of subgroups of $\mathbb{C}^\times$.

   - The set $\mathbb{R}^\times$ of non-zero real numbers.
   - The set $S = \{a + bi \in \mathbb{C} : a^2 + b^2 = 1\}$; S is the set of complex numbers of modulus 1, geometrically it is the unit circle in the complex plane. To see why S is a subgroup of $\mathbb{C}^\times$, you need to confirm that S is closed under multiplication and that it contains the inverse of each of its elements.

   Is the set of *pure imaginary* numbers a subgroup of $\mathbb{C}^\times$? Recall that a complex number is pure imaginary if its real part is zero and its imaginary part is not (e.g. $2i$, $3i$ etc.).

Let G be a group. It is usual to denote the result of combining elements a and b of G by ab (like a product). In the same way we can denote the element of combining a with a by a^2 (same as aa), hence we have a^3 $(= aaa)$, a^4 $(= aaaa)$, etc. We can think of these elements as "positive integer powers" of a.
We also adopt the convention that for every element a of G, a^0 is understood to be the identity element.
Also, a^{-1} is the inverse of a, and we may understand a^{-2} as $a^{-1}a^{-1}$, and so on: $a^{-1}, a^{-2}, a^{-3}, \ldots$ are the positive integer powers of a^{-1}.
Thus for any element a of G we have the full set of "integer powers" of a within G; moreover, they behave as we would like integer powers to behave in the sense that

$$a^r a^s = a^{r+s} \text{ for all } r, s \in \mathbb{Z}.$$

Note: We are not assuming that all of the integer powers of a are necessarily distinct.
Notation: The set of integer powers of an element a of G is often denoted by $\langle a \rangle$:

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, \mathrm{id}, a, a^2, a^3, \ldots\} = \{a^n : n \in \mathbb{Z}\}.$$

Lemma 1.3.3. *For a group* G *and any element* a *of* G, $\langle a \rangle$ *is a subgroup of* G.

Proof. We need to show that

1. $\langle a \rangle$ is closed under the group operation.
   This is clear, the elements of $\langle a \rangle$ are exactly those that have the form a^r for some integer r, and $a^r a^s = a^{r+s}$.

2. $\mathrm{id} \in \langle a \rangle$.
   This is true by definition, since $\mathrm{id} = a^0$.

3. $\langle a \rangle$ contains the inverse of each of its elements.
   To see this, note that for an integer r the inverse of a^r is a^{-r}.

□

Remark: We could have omitted Item 2. from the above proof. Why?

Definition 1.3.4. *$\langle a \rangle$ is called the* cyclic subgroup *of* G *generated by* $\langle a \rangle$.
In general, a subgroup of G *is said to be* cyclic *if it is equal to* $\langle a \rangle$ *for some* $a \in G$.

The proof of Lemma 1.3.3 above is very typical of proofs in group theory. The context is a completely abstract group about which we know nothing at all. The Lemma says that given any group, we can choose any element and the set of all powers of that element (and its inverse) in the group will give us a subgroup. We can now apply this lemma to examples, as in the following cases.

1. In $(\mathbb{Z}, +)$, the operation is addition, and the cyclic subgroup generated by 2 consists of all those elements that can be obtained by adding 2 (or its inverse -2) to itself repeatedly. This subgroup includes 2, $2+2=4$, $2+2+2=6$, etc. It also includes the identity element 0, the inverse -2 of 2, and the elements $(-2)+(-2)=-4$, $(-2)+(-2)+(-2)=-6$, etc.
   The cyclic subgroup of $\mathbb{Z}$ generated by 2 consists of all the even integers.
   Question: What is the cyclic subgroup of $\mathbb{Z}$ generated by 1? By 3?

2. In D_{2n}, let R denote the rotation through $\frac{2\pi}{n}$ about the centroid of the regular polygon. Then the cyclic subgroup generated by R is the group of rotational symmetries of the object. It has n elements.
   If S is one of the reflections in D_{2n} then S is its own inverse and the cyclic subgroup of D_{2n} generated by S consists only of S itself and of the identity element.

3. What are the elements of the cyclic subgroup of $\mathbb{C}^\times$ generated by -1?
   What are the elements of the cyclic subgroup of $\mathbb{C}^\times$ generated by i?
   Under what conditions on the complex number z is the subgroup $\langle z \rangle$ of $\mathbb{C}^\times$ a finite group?

Suppose that a is an element of a group G. Then any subgroup of G that contains a must also contain $a^2, a^3, \ldots$, and must also contain a^{-1} and hence $a^{-2}, a^{-3}, \ldots$ as well as the identity element. Hence any subgroup of G that contains the element a must contain $\langle a \rangle$, the cyclic subgroup generated by a. Sometimes it is helpful to think of $\langle a \rangle$ as the set of elements that *must* be in any subgroup that contains a.

Having discussed the concept of the cyclic subgroup of a group that is generated by a particular element, we now move on to the related idea of what it means for a group to be cyclic.

Definition 1.3.5. *A group* G *is said to be* cyclic *if* $G = \langle a \rangle$ *for some* $a \in G$.

Alternative version(s) of definition: A group G is cyclic if it contains an element a with the property that *every* element of G is a "power" of a. A cyclic group is one that is generated by a single element, in the sense that we can start with a single element and produce all the elements of G by (repeatedly) taking powers of that element and its inverse and by multiplying the results of such operations together.

In order to show that a group is cyclic, it is generally necessary to produce an example of a generator for it. It is generally not the case that any element (or any non-identity element) will do this job.

Examples

1. $(\mathbb{Z}, +)$ is an infinite cyclic group, with 1 as a generator.
   (This is saying that every integer is either equal to 0 (the identity in this group) or can be obtained by repeatedly adding 1 or -1 to itself).
   Question: There is one other element that is a generator for $(\mathbb{Z}, +)$ as a cyclic group. What is it?

2. For a natural number n, the group of nth roots of unity in $\mathbb{C}^\times$ is a cyclic group of order n, with (for example) $e^{\frac{2\pi i}{n}}$ as a generator. The elements of this group are the complex numbers of the form $e^{k\frac{2\pi i}{n}}$, where $k \in \mathbb{Z}$.
   Question to think about: What other elements generate this group? The answer to this question is slightly tricky and depends on n.

3. For $n \geqslant 3$, the group of rotational symmetries of a regular n-gon (i.e. a regular polygon with n sides) is a cyclic group of order n, generated (for example) by the rotation through $\frac{2\pi}{n}$ in a counterclockwise direction.

The term *order* appears in the examples above. Here's its definition.

Definition 1.3.6. *The* order *of a finite group is the number of elements in it. A group with infinitely many elements is said to have* infinite order.

It is common practice to denote a cyclic group of order n by C_n, and an infinite cyclic group by C_∞. We might write C_n as $\langle x \rangle$ and think of C_n as being generated by an element x. The elements of C_n would then be

$$\mathrm{id}, x, x^2, \ldots, x^{n-1}.$$

Here it is understood that $x^n = \mathrm{id}$, and that multiplication is defined by

$$x^i \cdot x^j = x^{[i+j]_n},$$

where $[i+j]_n$ denotes the remainder on dividing $i+j$ by n. In this context the multiplication table for $C_4 = \langle x \rangle$ is given below.

C_4	id	x	x^2	x^3
id	id	x	x^2	x^3
x	x	x^2	x^3	id
x^2	x^2	x^3	id	x
x^3	x^3	id	x	x^2

Note: The philosophy here is that all cyclic groups of order n (or 4) really look the same, so we might as well have one notation C_n for them. Once we give a name to a generator, like x, we can write out the multiplication table as for C_4 above. In this context, we don't care what sort of object x is, whether it is a number, a matrix, a function, a permutation or whatever. The group of nth roots of unity in $\mathbb{C}$ and the group of rotational symmetries of the regular n-gon might be regarded as particular manifestations of C_n in algebra and geometry. Later we will have the language to make all of this precise.

We might ask how many elements of C_n are actually generators of it as a cyclic group and how this number depends on n. The answer is not immediately obvious. Of course (provided $n > 1$) the identity element is never a generator of C_n and so the answer is at most $n - 1$. In the case of C_4, we can use the table above to look at the set of powers of each element and see if they include the whole group. We find

- Powers of x: x, x^2, x^3, id - the whole group.
- Powers of x^2: x^2 and id only - not the whole group.
- Powers of x^3: x^3, x^2, x, id - the whole group.

So two of the four elements of C_4 generate it as a cyclic group. What about C_5? What about C_6?

Theorem 1.3.7. *Suppose that* x *is a generator of* C_n. *Then the elements of* C_n *that generate it as a cyclic group are exactly those elements of the form* x^i *where* $\gcd(i, n) = 1$. *The number of these is* $\phi(n)$.

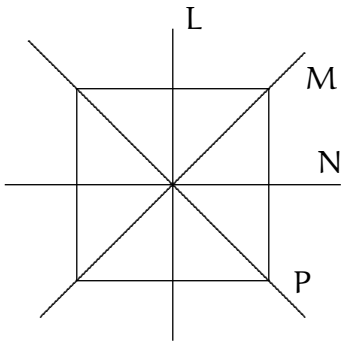
The proof is deferred for now, maybe until Problem Sheet 2.

Recall: For a natural number n, $\phi(n)$ is the number of integers in the range $1, \ldots, n$ that are relatively prime to n.

We finish this section by remarking that the cyclic subgroup generated by a particular element is a special case of a more general phenomenon. Suppose that G is a group and that S is a subset (not necessarily a subgroup) of G. Then we can define *the subgroup of* G *generated by* S. This is denoted by $\langle S \rangle$ and it consists of all the elements of G that can be obtained by starting with the identity and the elements of S and their inverses, and multiplying these elements together in all possible ways. So $\langle S \rangle$ is the smallest subgroup of G that contains S.

Definition 1.3.8. *If* $\langle S \rangle$ *is all of* G, *we say that* S *is a* generating set *of* G.

Problems As usual let D_8 denote the group of symmetries of the square (below).



Let S_L, S_M, S_N, S_P denote the reflections in the indicated lines, and let R_t denote the anticlockwise rotation through t°.

1. Show that the subgroup of D_8 generated by R_{180} and S_L is not all of D_8. (For example it does not contain R_{90}).

2. Show that D_8 can be generated by R_{90} and by any one of the reflections.

3. Show that $\{S_L, S_M\}$ is a generating set for D_8.

4. More generally, show that the group D_{2n} of symmetries of the regular n-gon can be generated by the counterclockwise rotation through $\frac{2\pi}{n}$ and any one reflection.
   This last one might be tricky - remember that by having the rotation through $\frac{2\pi}{n}$ in your generating set, you get all the rotations for free. What needs to be shown is that you can get all the reflections by composing the one reflection that is in your symmetry group with rotations. If in doubt, start with the equilateral triangle, the square and the regular pentagon.

Chapter 2

Essential concepts of group theory

2.1 Lagrange's Theorem

Recall the following terminology and notation. Suppose that a and b are natural numbers (positive integers). We say that a *divides* b if $b = ka$ for some integer k, i.e. if b is a multiple of a or equivalently if a is a factor of b.
Examples: 3 divides 12: $3|12$. However 3 does not divide 14: $s \not| 14$.
Note: Make sure you are using this language and notation accurately (many people don't). The statement "a divides b" means that a is a factor of b. It has nothing to do with the number "a divided by b". The written shorthand for this statement is $a|b$; the symbol in it is a vertical bar, it is not a forward slash or a backslash or a hyphen. In particular it has no connection to the slash that is used in fractions as in a/b.

The purpose of this section is to explore and prove the following theorem, known as Lagrange's Theorem. This theorem was not actually proved by Lagrange, but it was observed by him in 1771 the case of certain groups of permutations arising from his study of solutions of polynomial equations. It was proved in more generality by Gauss in 1801. We have already observed it in the examples of Section 2.3 when we looked at certain subgroups of the group of permutations of five letters.

Theorem 2.1.1 (Lagrange's Theorem)**.** *If* G *be a finite group and* H *is a subgroup of* G*, then the order of* H *divides the order of* G*.*

So for example, Lagrange's Theorem tells us that there is no point in looking for a subgroup with 7 elements in a group with 24 elements; no such subgroup exists.

The rest of this section will be devoted to a proof of Theorem 2.1.1, with some supporting examples and some new concepts that will be needed for the proof. It is not immediately obvious how we could possibly go about trying to prove this theorem, in the absence of any specific information about the groups in question. The fact that this can be done at all illustrates the power of the axiomatic approach to algebra. Nevertheless it is worth mentioning that the statement of Lagrange's Theorem was noticed for specific examples (by Lagrange) before being stated in a general context. New mathematical theory very frequently comes from observations about particular examples (that are later found to apply more generally) rather than reasoning with completely abstract concepts. However the finished product is often stated and described in terms of an abstract setting, so that it can be applied as widely as possible.

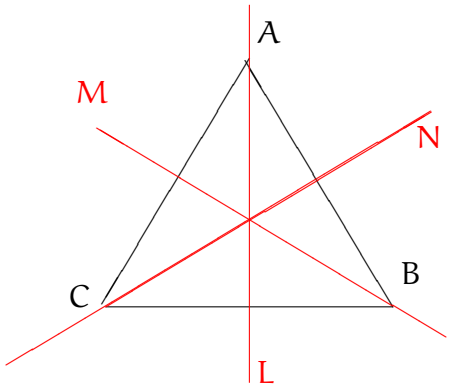
So how could we possibly go about proving that the order of a subgroup must be a factor of the order of the whole group? How can we even relate these two numbers when we are not talking about a specific example. The basic idea is to show that the whole group G can be represented as the union of a number of "shifted copies" of the subgroup H, in such a way that each copy has the same number of elements as H and every element of G belongs to exactly one of them. We are going to break the group into disjoint pieces each of which has the same number of elements as H and somehow "resembles" H. The pieces, or "shifted copies" are called *cosets*.

Definition 2.1.2. *Let* G *be a group and let* H *be a subgroup of* G*. Let* g *be an element of* G*. Then the* left coset *of* H *determined by* g *is defined to be the set*

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

Note: In the last line above, g is a specified element of G and h is running through all the elements of H. So gH is the subset of G consisting of those elements that can be obtained by multiplying an element of H on the left by g.

Example 2.1.3. *Let* D_6 *be the set of symmetries of the equilateral triangle, with rotations* id, R_{120}, R_{240} *and reflections* S_L, S_M *and* S_N *as shown.*



Then $H = \{\mathrm{id}, S_L\}$ *is a subgroup of* D_6 *of order 2, and left cosets of* H *in* D_6 *determined by the six elements are:*

1. $\mathrm{id}H = \{\mathrm{id} \circ \mathrm{id}, \mathrm{id} \circ S_L\} = \{\mathrm{id}, S_L\} = H$
2. $S_L H = \{S_L \circ \mathrm{id}, S_L \circ S_L\} = \{S_L, \mathrm{id}\} = H$ *again.*
3. $R_{120}H = \{R_{120} \circ \mathrm{id}, R_{120} \circ S_L\} = \{R_{120}, S_M\}$.
4. $S_M H = \{S_M \circ \mathrm{id}, S_M \circ S_L\} = \{S_M, R_{120}\} = R_{120}H$ *again.*
5. $R_{240}H = \{R_{240} \circ \mathrm{id}, R_{240} \circ S_L\} = \{R_{240}, S_N\}$
6. $S_N H = \{S_N \circ \mathrm{id}, S_N \circ S_L\} = \{S_N, R_{240}\} = R_{240}H$ *again.*

Note that there are only three distinct cosets (although each appears twice in the list). Each of these cosets has two elements (same as H) and every element of D_6 appears in exactly one of these three distinct cosets. It follows that the number of elements in D_6 is 3×2, which means in particular that it is a multiple of 2 which is what Lagrange's Theorem says. This example contains the key idea for our proof of Lagrange's Theorem, all we have to do is express the same idea in abstract terms and establish some properties of left cosets.

We have the following important observations.

Lemma 2.1.4. *Suppose* H *is a finite subgroup of a group* G *and that* $g \in G$*. Then* gH *has the same number of elements as* H*.*

Proof. Write k for the order of H and write $h_1, h_2, \ldots, h_k$ for the elements of H.
So the elements of gH are $gh_1, gh_2, \ldots, gh_k$. It looks like gH has k elements, to confirm this we just have to confirm that there is no repetition in this list. So suppose that $gh_i = gh_j$ for some i and j in the range $1, \ldots, k$. We can multiply both sides of this equation on the left by g^{-1} to deduce that this means $h_i = h_j$ and hence $i = j$. So the gh_i are distinct for $i = 1, \ldots, k$ and the coset gH has the same number of elements as H. □

Lemma 2.1.5. *Suppose that* g_1 *and* g_2 *are elements of* G *and that* H *is a subgroup of* G*. Then either the cosets* g_1H *and* g_2H *are equal to each other or they are disjoint from each other, i.e. their intersection is empty, they have no element in common.*

Note: Since g_1H and g_2H are *sets* (subsets of G). what it means to say that they are equal is that they contain exactly the same elements. A standard approach to presenting a proof that two sets A and B are equal is to show that every element of A belongs to B (so $A \subseteq B$) and that every element of B belongs to A (so $B \subseteq A$).

Proof. If g_1H and g_2H have no element in common then there is nothing to do. So suppose that these two sets *do* have at least one element in their intersection. This means that there are elements h_1 and h_2 of H for which

$$g_1h_1 = g_2h_2.$$

(To see this, note that elements of g_1H have the form g_1h where $h \in H$, and elements of g_2H have the form g_2h where $h \in H$. An element that belongs to both of these sets must simultaneously be equal to g_1h_1 and to g_2h_2, for some elements h_1, h_2 of H).

Now that g_1H and g_2H have non-empty intersection, we need to show that these sets must actually be equal. We can make use of the fact that H is a group. First we show that $g_1H \subseteq g_2H$.

Let $h \in H$. We want to show that $g_1h \in g_2H$. We know that $g_1 = g_2h_2h_1^{-1}$, so we can write

$$g_1 = g_2h_2h_1^{-1} \Longrightarrow g_1h = g_2h_2h_1^{-1}h = g_2(h_2h_1^{-1}h).$$

Now since H is closed under the operation of G and under taking inverses, we know that the element $h_2h_1^{-1}h$ belongs to H, and hence that g_1h belongs to the left coset g_2H. Thus $g_1H \subseteq g_2H$.

A similar argument, using the fact that $g_2 = g_1h_1h_2^{-1}$, shows that $g_2H \subseteq g_1H$. Hence $g_1H = g_2H$ as required. □

Lemma 2.1.5 says that two left cosets of a subgroup H in a group G are equal to each other if they intersect at all. This (and our proof above) applies to all groups not just finite groups. Note that the proof uses both the fact that H is closed under the group operation and the fact that it contains the inverse of each of its elements.

Lemma 2.1.6. *If* g *is an element of* G *and* H *is a subgroup of* G*, then* g *belongs to* some *left coset of* H *in* G.

Proof. For example, G belongs to the left coset gH, since $id_G \in H$. □

The significance of Lemma 2.1.6 is that it shows that the union of the various left cosets of H in G is the full group G.

We are now in a position to prove Lagrange's Theorem by putting all of these facts together in the context where G is a finite group. In this case we know that G is the union of the distinct left cosets of H, that each of these has the same number of elements, and that they don't intersect each other. So to count the elements of G we just need to add up the numbers in each coset - this is essentially the proof.

Theorem 2.1.1. *If* G *is a finite group and* H *is a subgroup of* G*, then the order of* H *divides the order of* G.

Note: We will use the notations $|G|$ and $|H|$ respectively for the orders of G and H. (This is standard in group theory).

Proof. Since G is a finite group there are finitely many left cosets of H in G. Let $H, g_2H, \ldots, g_kH$ be the *distinct* left cosets of H in G. (We have seen that two elements of G may determine the same left coset - what the word *distinct* here means is that each coset is counted only once. By Lemma 2.1.4, each of these cosets has exactly $|H|$ elements. By Lemmas 2.1.5 and 2.1.6, each element of G appears in exactly one of them. Thus the number of elements of G is

$$\underbrace{|H| + |H| + \cdots + |H|}_{k} = k|H|.$$

So the order of G is an integer multiple of H. □

Definition 2.1.7. *If* H *is a subgroup of a finite group* G*, then the integer* $|G|/|H|$ *is called the* index *of* H *in* G *and denoted by* $[G : H]$.

2.2 The centre, centralizers and conjugacy

Definition 2.2.1. *Let* G *(or* $(G, \star)$ *be a group. The* centre *of* G*, denoted by* $Z(G)$ *is the subset of* G *consisting of all those elements that commute with* every *element of* G*, i.e.*

$$Z(G) = \{x \in G : x \star g = g \star x \text{ for all } g \in G\}.$$

For example, the centre of G is equal to G if and only if G is abelian.

Example 2.2.2. *What is the centre of* $GL(n, \mathbb{Q})$*, the group of* $n \times n$ *invertible matrices with rational entries (under matrix multiplication)?*

Solution (Summary): Suppose that A belongs to the centre of $GL(n, \mathbb{Q})$ (so A is a $n \times n$ invertible matrix). For i, j in the range $1, \ldots, n$ with $i \neq j$, let E_{ij} denote the matrix that has 1 in the (i, j) position and zeros in all other positions. Then $I_n + E_{ij} \in GL(n, \mathbb{Q})$ and

$$A(I_n + E_{ij}) = (I_n + E_{ij})A \Longrightarrow A + AE_{ij} = A + E_{ij}A \Longrightarrow AE_{ij} = E_{ij}A.$$

Now AE_{ij} has Column i of A as its jth column and is otherwise full of zeros, while $E_{ij}A$ has Row j of A as its ith row and is otherwise full of zeros. In order for these two matrices to be equal for all i and j, it must be that the off-diagonal entries of A are all zero and that the entries on the main diagonal are all equal to each other. Thus $A = aI_n$, for some $a \in \mathbb{Q}$, $a \neq 0$. On the other hand it is easily checked that any matrix of the form aI_n where $a \in \mathbb{Q}$ *does* commute with all other matrices. Hence the centre of $GL(n, \mathbb{Q})$ consists precisely of those matrices aI_n where $a \in \mathbb{Q}$, $a \neq 0$.
Note: Matrices of this form are called *scalar* matrices, they are scalar multiples of the identity matrix.
Exercise: Write out an expanded version of the above proof yourself, making sure that you follow all the details. Proofs like this that involve matrix indices and the mechanism of matrix multiplication tend to be fairly concise to write down but also fairly intricate for the reader to unravel.

A key fact about the centre of a group is that it is not merely a subset but a *subgroup*.

Theorem 2.2.3. *Let* G *be a group. Then* $Z(G)$ *is a subgroup of* G*.*

Proof. We have the usual three things to show, and we must use the definition of the centre to show them.

- $Z(G)$ is closed under the operation of G.
  Suppose $a, b \in Z(G)$. We must show that $ab \in Z(G)$. That means showing that for any element x of G, x commutes with ab. Now

  $$\begin{aligned} abx &= axb \ (bx = xb \text{ since } b \in Z(G)) \\ &= xab \ (ax = xa \text{ since } a \in Z(G)). \end{aligned}$$

  So $abx = xab$ for all $x \in G$, and $ab \in Z(G)$.

- $id_G \in Z(G)$
  By definition $id_G x = x id_G = x$ for all $x \in G$, so id_G commutes with every element of G and belongs to the centre of G.

- Suppose $a \in Z(G)$. We need to show that $a^{-1} \in Z(G)$.
  Let x in$G$. Then

  $$ax = xa \Longrightarrow axa^{-1} = xaa^{-1} = x \Longrightarrow a^{-1}axa^{-1} = a^{-1}x \Longrightarrow xa^{-1} = a^{-1}x.$$

  Thus a^{-1} commutes with x for all $x \in G$ and $a^{-1} \in Z(G)$.

We conclude that $Z(G)$ is a subgroup of G. □

Exercise: Show that $Z(D_6)$ is the trivial subgroup.

Another important concept in group theory is introduced in the next definition.

Definition 2.2.4. *: Let* G *be a group and let* $g \in G$*. A* conjugate *of* g *in* G *is an element of the form* xgx^{-1} *for some* $x \in G$*. The set of* all *conjugates of* g *in* G *is called the* conjugacy class *of* G*.*

It may not be immediately obvious why this notion of conjugacy is an important one. Basically elements that are conjugates of each other have many properties in common (we will see in the next chapter what this means in the special case of groups of permutations). To get a sense of what the definition means we will start with a few observations.

1. Think of the element g as being fixed and imagine that we are looking at the various conjugates of g. These are the elements xgx^{-1} where $x \in G$. The element xgx^{-1} is equal to g if and only if $gx = xg$, i.e. if and only if x commutes with g.
2. This means that if every element of G commutes with g (i.e. if $g \in Z(G)$), then all the conjugates of g are equal to g, and the conjugacy class of g consists only of the single element g.
3. In particular this means that if G is abelian, then every conjugacy class in G consists of a single element (this is not really an interesting case for the concept of conjugacy).
4. So (roughly) the number of distinct conjugates of an element G measures how far away it is from being in the centre. If an element has few conjugates then it commutes with many elements of the group. If an element has many conjugates, it commutes with few elements. We will make this precise later.
5. Every element g of G is conjugate to itself, since for example $g = ggg^{-1}$.

Example 2.2.5. *Let the elements of* D_8*, the group of symmetries of the square, be denoted by* $\mathrm{id}, R_{90}, R_{180}, R_{270}$ *(the rotations),* S_L, S_M *(the reflections in the perpendicular bisectors of the sides), and* S_N, S_P *(the reflections in the two diagonals). Then* D_8 *has five distinct conjugacy classes as follows:*

$$\{\mathrm{id}\},\ \{R_{180}\},\ \{R_{90}, R_{270}\},\ \{S_L, S_M\},\ \{S_N, S_P\}.$$

This is saying that:

- $\{\mathrm{id}\}$ and R_{180} are in the centre.
- R_{90} and R_{270} are conjugate to each other. To confirm this, look at (for example) the element $S_L \circ R_{90} \circ S_L^{-1}$ and confirm that it is equal to R_{270}. You can replace S_L with any of the reflections here, they will all work.
- The reflections S_L and S_M are conjugate to each other. To confirm this you could look at $S_N \circ S_M \circ S_N^{-1}$.
- The reflections S_N and S_P in the diagonals are conjugate to each other. To confirm this you could look at $S_M \circ S_N \circ S_M^{-1}$.

Note that in this case the whole group is the union of the distinct conjugacy classes, and that different conjugacy classes do not intersect each other. This is a general and important feature of groups. We will not prove it formally although you are encouraged (as an exercise) to adapt the following description to a formal proof. If two elements of G are conjugate to each other, then any element that is conjugate to either of them is conjugate to both. Thus the conjugacy class of an element g is the same as the conjugacy class of hgh^{-1} for any $h \in G$. On the other hand, if two elements are not conjugate to each other, then no element can be simultaneously conjugate to both of them, and their conjugacy classes do not intersect.

In the case of D_8 above, we can notice that the numbers of elements in the conjugacy classes (1,1,2,2 and 2) are all factors of the group order which is 8. We will finish Chapter 2 now by showing that this is not an accident.

Definition 2.2.6. *Let* g *be an element of a group* G*. Then the* centralizer *of* g *in* G*, denoted* $C_G(g)$*, is defined to be the set of all elements of* G *that commute with* g*, i.e.*

$$C_G(g) = \{x \in G : xg = gx\}.$$

Theorem 2.2.7. *For every* $g \in G$*,* $C_G(g)$ *is a subgroup of* G*.*

The proof of Theorem 2.2.7 is a problem on Problem Sheet 2.
Two observations about centralizers:

1. The centralizer of g in G is equal to G if and only if $g \in Z(G)$.
2. For an element g of G that is not in the centre, $C_G(g)$ will be a subgroup that contains both $Z(G)$ and g (and so properly contains $Z(G)$) but is not equal to G.

The following theorem relates the centralizer of an element g of G to the conjugacy class of g. It is a special case of the famous Orbit-Stabilizer Theorem concerning group actions.

Theorem 2.2.8. *Let* g *be an element of a finite group* G*. Then the number of distinct conjugates of* g *is* $[G : C_G(x)]$*, the index in* G *of* $C_G(g)$*.*

Note: Using Example 2.2.5 above, we can verify this theorem for the dihedral group D_8.

It is convenient to mention the following necessary Lemma first, rather than trying to prove it in the middle of the proof of Theorem 2.2.8.

Lemma 2.2.9. *Suppose that* H *is a subgroup of a finite group* G*. Let* x, y *be elements of* G*. Then the cosets* xH *and* yH *are equal if and only if the element* $y^{-1}x$ *belongs to* H*.*

Proof. From Lemma 2.1.5 we know that xH and yH are equal if and only if $x \in yH$ (since in this case x belongs to both xH and yH and the cosets are equal since they intersect). This occurs if and only if $x = yh$ for some $h \in H$, if and only if $y^{-1}x = h$, i.e., if and only if the element $y^{-1}x$ belongs to H. □

Proof. Recall that $[G : C_G(x)]$ is the number of left cosets of $C_G(g)$ in G. We will show that two elements of G determine distinct conjugates of g if and only if they belong to distinct left cosets of $C_G(g)$. To see this let x_1 and x_2 be elements of G. Then

$$\begin{aligned} x_1 g x_1^{-1} &= x_2 g x_2^{-1} \\ \iff g x_1^{-1} &= x_1^{-1} x_2 g x_2^{-1} \\ \iff g x_1^{-1} x_2 &= x_1^{-1} x_2 g \\ \iff x_1^{-1} x_2 &\in C_G(g) \end{aligned}$$

By Lemma 2.2.9, this occurs if and only if the cosets $x_1 C_G(g)$ and $x_2 C_G(g)$ are equal. Thus elements of G determine distinct conjugates of g if and only if they belong to distinct left cosets of $C_G(g)$, and the number of distinct conjugates of g is the number of distinct left cosets of $C_G(g)$ in G, which is $[G : C_G(g)]$. □

In particular, since $|G| = |C_G(g)|\,[G : C_G(g)]$, the number of elements in each conjugacy class of G is a factor of G. This fact can be used to prove the following important theorem about finite p-groups. A finite p-group is a group whose order is a power of a prime p (e.g. a group of order 27, 64, or 125).

Theorem 2.2.10. *Suppose that* G *is a finite* p*-group. Then the centre of* G *cannot be trivial, i.e. it cannot consist only of the identity element.*

Proof. As an example, suppose that $p = 5$ and that $|G| = 5^4 = 625$. (As an exercise you could adapt the proof for this example to a general proof). Suppose that the conjugacy classes of G are C_1, C_2 dots, C_k. Remember that every element of the centre comprises a conjugacy class all on its own, and that each non-central element belongs to a conjugacy classes whose number of elements is greater than 1 and is a divisor of 5^4. Suppose that C_1 is the conjugacy class that consists only of the identity element. Then

$$|G| = 5^4 = 1 + |C_2| + |C_3| + \cdots + |C_k|.$$

(This is called the *class equation* of G). Each $|C_i|$ is either 1 or a multiple of 5. If all of $|C_2|, |C_3|, \ldots, |C_k|$ are multiples of 5, it means that $|G| = 1 +$ (a multiple of 5), so $|G|$ would have remainder 1 on division by 5. This is not possible since $|G| = 5^4$, so it must be that some (at least 4) of the C_i (apart from C_1) consist of a single element. These "single element" conjugacy classes correspond to non-identity elements of the centre of G. □

Chapter 3

The symmetric groups

3.1 Working with elements of symmetric groups

Definition 3.1.1. *The group consisting of all permutations of a set of* n *elements is called the* symmetric group of degree n *and denoted* S_n.

REMARKS

1. The order of S_n is $n!$, the number of permutations of n objects.
2. We often think of the n elements being permuted as the first n positive integers $1, 2, \ldots, n$, but this is not intrinsic to the definition of S_n. It doesn't really matter what these elements are called as long as they have distinct labels.
3. Although the terminology is potentially problematic, it is important not to confuse the term "symmetric group" with groups of symmetries of (for example) regular polygons.

This section is mostly about how to represent permutations and how to do calculations with them. Later in the chapter we will use this information to deduce some nice properties of the symmetric groups.

An element of S_4 is a permutation of the set $\{1, 2, 3, 4\}$; this means a function from that set to itself that sends each element to a different image, and hence shuffles the four elements. In S_4, a basic way to represent the permutation $1 \to 1,\ 2 \to 4,\ 3 \to 2,\ 4 \to 3\}$ is by the array

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}.$$

Representing permutations like this we can practise multiplying (or composing) them. In these notes we will use the convention that for permutations σ and τ, the product $\sigma\tau$ means "σ after τ or $\sigma \circ \tau$, i.e. that the factor that is written on the right is applied first. This is not a universally agreed convention and people use both possible interpretations. For this course it is probably a good idea that we all share the same interpretation to avoid confusion, but in general all that is important is that you state in which order you are considering the composition to take place and that you are consistent.

Example 3.1.2. *In* S_5, *suppose that*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}.$$

Calculate the products $\sigma\tau$ *and* $\tau\sigma$.

Solution: To calculate $\sigma\tau$, we apply τ first and then σ. Remember that this is just a composition of functions.

- τ sends 1 to 4, then σ sends 4 to 4. So $\sigma\tau$ sends 1 to 4.
- τ sends 2 to 2, then σ sends 2 to 3. So $\sigma\tau$ sends 2 to 3.
- τ sends 3 to 3, then σ sends 3 to 5. So $\sigma\tau$ sends 3 to 5.
- τ sends 4 to 5, then σ sends 5 to 1. So $\sigma\tau$ sends 4 to 1.
- τ sends 5 to 1, then σ sends 1 to 2. So $\sigma\tau$ sends 5 to 2.

We conclude that

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$$

You would not be expected to provide all this detail in every example like this, it is provided here to explain how the process works. It's a good idea to practise this so that you can do the calculation in one line. The answer to the second part is

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

This array format is not the only way of representing a permutation and not always the most useful way. Another way of thinking about a permutation π is by thinking about how it moves the elements of the set around, by starting with a single element and following what happens when you repeatedly apply π to it and look at the sequence of images. Eventually you will have to get back to the original element. Consider the following example in S_{14}.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 11 & 9 & 8 & 2 & 5 & 1 & 12 & 14 & 6 & 7 & 3 & 13 & 10 & 4 \end{pmatrix}$$

Start with the element 1 and look at what happens to it when you repeatedly apply π.

- First you get $1 \to 11$;
- Then $11 \to 3$;
- Then $3 \to 8$;
- Then $8 \to 14$;
- Then $14 \to 4$;
- Then $4 \to 2$;
- Then $2 \to 9$;
- Then $9 \to 6$;
- Then $6 \to 1$.

After ten applications of π we arrive back at 1 and this is the first time we have a repetition in the list. This will happen every time: the list can't continue indefinitely without repetition because there are only finitely many elements being permuted. Suppose that after starting at 1 the first repetition occurs at Step k, after k applications of π. Then we have

$$1 \to a_1 \to a_2 \to \cdots \to a_{k-1} \to$$

where $1, a_1, \ldots, a_{k-1}$ are distinct. The next element (a_k) is a repeat of one of these. However it can't be a repeat of a_1, because 1 is the only element whose image under π is a_1, and $a_{k-1} \neq 1$. The same applies to $a_2, \ldots, a_{k-1}$. So it must be that 1 (the element where we started) is the first element to be repeated, and that we close the circle that started with 1. In our example above

there were nine distinct elements in the sequence that started at 1. So the permutation π produces the following *cycle*:

$$1 \to 11 \to 3 \to 8 \to 14 \to 4 \to 2 \to 9 \to 6 \to 1$$

This cycle is often written using the following notation:

$$(1\ \ 11\ \ 3\ \ 8\ \ 14\ \ 4\ \ 2\ \ 9\ \ 6).$$

Note that 1 is not written at the end here. The above notation means the permutation (of 14 elements in this case) that sends 1 to 11, 11 to 3, etc, and sends 6 back to 1 at the end. There is nothing in the notation to indicate that we are talking about an element of S_{14} - this has to be clear from the context. Also, it is understood that elements that are not mentioned in the above notation are fixed by the permutation that it denotes. The permutation $(1\ 11\ 3\ 8\ 14\ 4\ 2\ 9\ 6)$ is an example of a *cycle of length 9* in S_{14}. It is not the same as the permutation π that we started with, but it does coincide with π on the set of nine elements that can be obtained by starting at 1 and repeatedly applying π. This set is called the *orbit* of 1 under π.

The point of this discussion is that π can be written as a product of *disjoint* cycles in S_{14}. The next step towards doing so is to look for the first element (in the natural order) of our set that is not involved in the first cycle. This is 5. Go back to π and see what happens to 5 under repeated application of π. We find that

$$5 \to 5,$$

so 5 is fixed by π. We could think of this as a cycle of length 1.

There are still some elements unaccounted for. The first one is 7. Looking at the orbit of 7 under π, we find

$$7 \to 12 \to 13 \to 10 \to 7$$

so we get the cycle $(7\ \ 12\ \ 13\ \ 10)$ of length 4. Note that this has no intersection with the previous cycles.

Our conclusion is that π can be written as the product of these disjoint cycles:

$$\pi = (1\ \ 11\ \ 3\ \ 8\ \ 14\ \ 4\ \ 2\ \ 9\ \ 6)(7\ \ 12\ \ 13\ \ 10).$$

If you like you can explicitly include (5) as a third factor, but the usual convention is not to bother including elements that are fixed in expressions of this nature, if an element does not appear it is understood to be fixed.

Notes

1. The representation of π in "array" format can easily be read from its representation as a product of disjoint cycles. For example if you want to know the image of 8 under π, just look at the cycle where 8 appears - its image under π is the next element that appears after it in that cycle, 14 in this example. If your element is written at the end of a cycle, like 10 in this example, then its image under π is the number that is written in the first position of that same cycle (so $10 \to 7$ here). An element that does not appear in any of the cycles is fixed by the permutation.

2. The statement above says that π can be effected by first applying the cycle $(7\ \ 12\ \ 13\ \ 10)$ (which only moves the elements $7, 12, 13, 10$) and then applying the cycle $(1\ 11\ 3\ 8\ 14\ 4\ 2\ 9\ 6)$ (which only moves the elements $1, 11, 3, 8, 14, 4, 2, 9, 6$). Since these two cycles operate on disjoint sets of elements and do not interfere with each other, they commute with each other under composition - it does not matter which is written first in the expression for π as a product of the two of them. So we could equally well write

$$\pi = (7\ \ 12\ \ 13\ \ 10)(1\ \ 11\ \ 3\ \ 8\ \ 14\ \ 4\ \ 2\ \ 9\ \ 6).$$

3. The expression for a permutation as a product of disjoint cycles is unique up to the order in which the cycles are written. This means that the same cycles must appear in any such expression for a given permutation, but they can be written in different orders.

   It might also be worth mentioning that a given cycle can be written in slightly different ways, since it doesn't matter which element is taken as the "starting point". For example $(7\ 12\ 13\ 10)$ and $(13\ 10\ 7\ 12)$ represent the same cycle.

Definition 3.1.3. *The expression of an element of S_n as a product of disjoint cycles partitions the set $\{1, 2, \ldots, n\}$ into disjoint* orbits. *In the above example there are three orbits:*

$$\{1, 2, 3, 4, 6, 8, 11, 14\},\ \{5\},\ \{7, 10, 12, 13\}.$$

If two elements belong to the same orbit for a permutation π, it means that some power of π takes one of those elements to the other. Note that fixed points *do* count as orbits. So the identity element of S_n has n orbits each consisting of a single element. A permutation in S_n has a single orbit if it is a single cycle involving all n elements.

It is good idea to practise moving between the "array representation" and "disjoint cycle representation" of a permutation. There is another way of representing permutations that is sometimes useful. We could think of the "simplest" type of non-identity permutation as being one that just swaps two elements and leaves the rest fixed. Such a permutation is called a transposition. The transposition that (for example) interchanges 1 and 2 and leaves all the other elements fixed is denoted, in typical cycle notation, as $(1\ 2)$.

Theorem 3.1.4. *Every element of S_n can be expressed as a product of transpositions.*

Rather than giving a formal general proof of Theorem 3.1.4, we will look at a way of expressing a given permutation as a product of transpositions. This contains all that would be required for a proof, without having to worry about setting up cumbersome general notation.

Example 3.1.5. *In S_8 (for example), the cycle $(2\ 4\ 7\ 6\ 8)$ can be written as the product*

$$(2\ 8)(2\ 6)(2\ 7)(2\ 4)$$

of four transpositions.

To see this, just look at what happens to each element under the proposed composition of transpositions. Start with 2. We have:

$$2 \to 4.$$

Move on to 4:

$$4 \to 2 \to 7.$$

Then 7:

$$7 \to 2 \to 6.$$

Then 6:

$$6 \to 2 \to 8.$$

Finally 8:

$$8 \to 2.$$

So overall our composition of transpositions amounts to the cycle

$$2 \to 7 \to 6 \to 8 \to 2,$$

as we wanted.

Note: The expression for a given cycle (or permutation) as a product of transpositions is *not unique*. For example we could write the 4-cycle above equally well as $(4\ 7\ 6\ 8\ 2)$, then using the same technique to write it as a product of transpositions would result in

$$(4\ 2)(4\ 8)(4\ 6)(4\ 7),$$

which does not involve the same transpositions as our example above, although it is the same permutation.

Example 3.1.6. *In S_{12}, write the element*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 11 & 4 & 6 & 1 & 10 & 7 & 8 & 12 & 9 & 3 & 2 & 5 \end{pmatrix}$$

as a product of transpositions.

Solution: First write it as a product of disjoint cycles.

$$(1\ 11\ 2\ 4)(3\ 6\ 7\ 8\ 12\ 5\ 10).$$

Then as a product of transpositions:

$$(1\ 4)(1\ 2)(1\ 11)(3\ 10)(3\ 5)(3\ 12)(3\ 8)(3\ 7)(3\ 6).$$

This expression involves 10 transpositions.

Exercise 3.1.7. *How many of the $n!$ elements of S_n are transpositions? How many are 3-cycles? (i.e. cycles of length 3, like $(1\ 2\ 3)$).*

The number of transpositions involved in an expression for a permutation as a product of transpositions is not uniquely determined either, since for example $(2\ 3)$ and $(1\ 3)(2\ 3)(1\ 2)$ are the same permutation. However, it *is* true that no permutation can be written both as the product of an even number and an odd number of permutations. To prove this is not difficult but involves a bit of fussing. This is our next task.

Theorem 3.1.8. *A permutation in S_n cannot be expressed both as the product of an even number and an odd number of transpositions.*

Let $\pi \in S_n$, and suppose that

$$\pi = \tau_s \tau_{s-1} \dots \tau_2 \tau_1,$$

where each τ_i is a transposition. Let r be the number of orbits of π (i.e. the number of cycles in the expression for π as a product of disjoint cycles, including fixed points). Then r is fully determined by π and so is $n - r$. We will show that s (the number of transpositions in our expression for π as a product of transpositions) has the same parity as $n - r$, i.e. that these numbers are both even or both odd.

We will do this by induction on s, the starting point being $s = 0$. If $s = 0$ then π is the identity permutation, $r = n$ and $n - r = 0$. So in this case s and $n - r$ are both zero, they are both even.

The case $s = 1$ is also manageable. If $s = 1$, then π is a single transposition, so it has one cycle of length 2 and $n - 2$ fixed points. In this case $r = n - 1$ and $n - r = 1$, so s and $n - r$ are both equal to 1, they are both odd.

Now suppose that s and $n - r$ have the same parity for all values of s up to $s = k$, and consider the case $s = k + 1$. This means

$$\pi = \tau_{k+1} \tau_k \dots \tau_2 \tau_1,$$

where each τ_i is a transposition. Let $\tau_{k+1} = (1\ 2)$ (there is no loss of generality here really) and let π' be the element of S_n given by

$$\pi' = \tau_k \dots \tau_2 \tau_1,$$

and let r' be the number of orbits of π'. We will show that the number r of orbits of π differs from r' by 1.

Case 1: Suppose first that 1 and 2 belong to the same orbit in π', and write the cycle corresponding to this orbit as $(1\ a_2 \dots a_l\ 2\ a_{l+m} \dots a_m)$. Then we have (check this)

$$(1\ 2)(1\ a_1 \dots\ a_l\ 2\ a_{l+1} \dots a_m) = (1\ a_1 \dots a_1)(2\ a_{l+1} \dots a_m).$$

So the orbit of π' that contained the elements 1 and 2 is split into two separate orbits by the multiplication by τ_{k+1}. Other orbits of π' are unaffected since they do not involve 1 or 2. So in the case where 1 and 2 belong to the same orbit of π', we have $r = r' + 1$.

Case 2: Suppose that 1 and 2 belong to different orbits of π', and write the cycles corresponding to these orbits as

$$(1\ a_1 \dots a_l),\ \ (2\ b_1 \dots b_m)$$

where none of the a_i is equal to any of the b_j. Then (check that)

$$(1\ 2)(1\ a_1 \dots a_l)(2\ b_1 \dots b_m) = (1\ a_1 \dots a_l\ 2\ b_1 \dots b_m),$$

so the effect of the multiplication by $(1\ 2)$ is to combine these two orbits into one. As in Case 1 there is no effect on the other orbits of π'. So in the case where 1 and 2 belong to different orbits of π', we have $r = r' - 1$.

By our induction hypothesis, $n-r'$ has the same parity as k. The above argument above shows that $n - r$ differs from $n - r'$ by 1, and hence it must have the same parity as $k + 1$ which is the number of transpositions in π.

We have proved that the parity (oddness or evenness) of the number of transpositions in any expression for π as a product of transpositions is the same as the parity of $n - r$. In particular, for a given π, this number of transpositions is always even or always odd.

Definition 3.1.9. *An element of S_n is called* even *if it can be written as the product of an even number of transpositions, and* odd *if it can be written as the product of an odd number of transpositions. Every element of S_n is either even or odd (not both).*

Note that the inverse of an even permutation is again even (it involves the same transpositions listed in the opposite order), and that the product of two even permutations is even. Moreover, the identity permutation is even, since it can be written as the "product of zero transpositions" or as the square of any transposition. Thus the set of *even permutations* of n objects is a subgroup of S_n. This is known as the *alternating group* of degree n and denoted by A_n. Directly counting the even permutations of a set of n elements is a more difficult task than counting *all* the permutations. However, by showing that the even permutations can be put in one-to-one correspondence with the odd permutations, we can show that exactly half of all the elements of S_n are even.

Theorem 3.1.10. *The order of the alternating group A_n is $\dfrac{n!}{2}$.*

Proof. Let the numbers of even and odd permutations in S_n be k_1 and k_2 respectively, and let τ denote the transposition $(1\ 2)$. For every even permutation π, we have a corresponding odd permutation $\pi\tau$. Thus there are at least as many odd permutations as even permutations, $k_1 \leqslant k_2$.

On the other hand, for every *odd* permutation σ we have the corresponding *even* permutation $\sigma\tau$. So there are at least as many even permutations as odd permutations, $k_2 \leqslant k_1$.

It follows that $k_1 = k_2$ and hence that the even permutations and odd permutations each account for half of all permutations. Thus

$$|A_n| = \frac{n!}{2}.$$

□

3.2 Conjugacy in S_n

A definition that we have sort of been using but that hasn't been stated yet is that of the *order* of an element of a group. Try not to confuse this with the order of the group itself.

Definition 3.2.1. *Let* G *be a group and let* $g \in G$. *The* order *of the element* g *is the least positive integer* k *for whcih* g^k *is the identity element. If no such* k *exists,* g *is said to have* infinite order. *The order of* g *is the order of the cyclic subgroup generated by* G.

So, for example, the order of each of the (non-identity) rotations of D_6 is 3, and the order of each reflection in any dihedral group is 2. The order of the identity element is always 1.

In a symmetric group, the order of a *cycle of length* k (also called a k-cycle) is k. This is because the cycle must be applied k times in order to map every element to itself and so obtain the identity permutation. In order to determine the order of a general element of S_n, look at its expression as a product of disjoint cycles. The order of the element is the least common multiple of the lengths of the disjoint cycles that appear in it.

Example 3.2.2. *What is the order of the element*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 2 & 8 & 5 & 1 & 3 & 7 \end{pmatrix}?$$

Solution: Look at the expression for π as a product of disjoint cycles:

$$\pi = (1\ 6)(2\ 4\ 8\ 7\ 3).$$

We see that π is the product of a cycle of length 2 and a cycle of length 5. If $\pi^k = \mathrm{id}$ for some integer k, then k must be even, since the kth power of the transposition $(1\ 6)$ must be the identity. Also k must be a multiple of 5, since the kth power of the 5-cycle $(2\ 4\ 8\ 7\ 3)$ must be the identity element. We conclude that the order of π is $\mathrm{lcm}(2,5) = 10$.

One nice property of the symmetric groups is that their conjugacy classes are easy to describe. We will say that two elements of S_n have the *same cycle type* if, when written as products of disjoint cycles, they both involve the same number of 1-cycles, the same number of 2-cycles, the same number of 3-cycles, and so on. For example, in S_{12}, the permutations

$$(1\ 4\ 3\ 5\ 11)(7\ 8\ 9) \text{ and } (2\ 8\ 7\ 12\ 3)(1\ 11\ 9)$$

both have the same cycle structure. Each of them involves one 5-cycle, one 3-cycle and four fixed points (1-cycles).

Theorem 3.2.3. *Let* $\pi = (a_1\ a_2 \dots\ a_k)$ *be a cycle of length* k *in* S_n, *and let* σ *be any permutation in* S_n. *Then the conjugate* $\sigma\pi\sigma^{-1}$ *is the cycle* $(\sigma(a_1)\ \sigma(a_2) \dots \sigma(a_k))$.

Proof. (more or less) We will see how this works for the particular example where $n = 7$, $k = 5$, $\pi = (1\ 2\ 3\ 4\ 5)$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 6 & 3 & 5 & 1 & 4 \end{pmatrix}$.

We want to consider the permutation $\sigma\pi\sigma^{-1}$. The elements 1 and 4 are sent by σ^{-1} to 6 and 7, which are not moved by π, and then mapped respectively back to 1 and 4 by σ.

So 1 and 4, which are the images under σ of the fixed points of π, are not moved by $\sigma\pi\sigma^{-1}$.

Now look at what happens to $2, 7, 6, 3, 5$ which are, respectively, the images under σ of the elements $1, 2, 3, 4, 5$ that are cycled (in that order) by π. First, σ^{-1} sends $2, 7, 6, 3, 5$ to $1, 2, 3, 4, 5$ respectively. Then π cycles these around, sending the list $1, 2, 3, 4, 5$ to $2, 3, 4, 5, 1$. Then σ maps the list $2, 3, 4, 5, 1$ back to $7, 6, 3, 5, 1$. So overall, the element $\sigma\pi\sigma^{-1}$ sends $2 \to 7$, $7 \to 6$, $6 \to 3$, $3 \to 5$ and $5 \to 2$. Thus this element is the cycle $(2\ 7\ 6\ 3\ 5)$, which is exactly $(\sigma(1)\ \sigma(2)\ \sigma(3)\ \sigma(4)\ \sigma(5))$, where $\pi = (1\ 2\ 3\ 4\ 5)$. □

Theorem 3.2.3 has the following important consequence.

Theorem 3.2.4. *Let π be any permutation in S_n. Then every conjugate of π in S_n has the same cycle type has π.*

Proof. Let $\pi_1, \ldots, \pi_k$ be the disjoint cycles in π, and suppose that σ is an element of S_n and we want to look at the conjugate $\sigma\pi\sigma^{-1}$ of π. Now

$$\pi = \pi_1\pi_2 \ldots \pi_k$$

and

$$\begin{aligned} \sigma\pi\sigma^{-1} &= \sigma\pi_1\pi_2 \ldots \pi_k\sigma^{-1} \\ &= \sigma\pi_1\sigma^{-1}\,\sigma\pi_2\sigma^{-1} \ldots \sigma\pi_k\sigma^{-1}. \end{aligned}$$

By Theorem 3.2.3, $\sigma\pi_i\sigma^{-1}$ is the cycle of the same length as π_i, that cycles the images under σ of the elements that are cycled by π_i. Since the images under σ of the disjoint orbits of π are still disjoint,

$$\sigma\pi_1\sigma^{-1}\,\sigma\pi_2\sigma^{-1} \ldots \sigma\pi_k\sigma^{-1}$$

is exactly the expression for $\sigma\pi\sigma^{-1}$ as a product of disjoint cycles. It has the same cycle type as π, since for each i, $\sigma\pi_i\sigma^{-1}$ is a cycle of the same length as π_i. □

The last part of this story is that if two elements of S_n have the same cycle type, then they *are* conjugate to each other in S_n. Theorem 3.2.4 and its proof show how to establish this. Again we will do it by example. Suppose you want to show that the elements π_1 and π_2 are conjugate to each other in S_8, where

$$\pi_1 = (1\,3\,4)(5\,6), \quad \pi_2 = (4\,8\,7)(1\,2).$$

Then π_1 and π_2 have the same cycle type obviously. Theorem 3.2.4 says that for any $\sigma \in S_8$,

$$\sigma\pi_1\sigma^{-1} = (\sigma(1)\ \sigma(3)\ \sigma(4))(\sigma(5)\ \sigma(6)).$$

If we want this to be equal to π_2 we should choose σ so that

$$\sigma(1) = 4,\ \sigma(3) = 8,\ \sigma(4) = 7,\ \sigma(5) = 1,\ \sigma(6) = 2.$$

For $\sigma(2),\ \sigma(7)$ and $\sigma(8)$ we can do whatever we like (amongst the availalbe options). If we choose

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 8 & 7 & 1 & 2 & 5 & 6 \end{pmatrix}$$

Then we have $\sigma\pi_1\sigma^{-1} = \pi_2$, as required.

Our conclusion is the following theorem.

Theorem 3.2.5. *Two elements of S_n are in the same conjugacy class if and only if they have the same cycle type.*

This means that the number of conjugacy classes in S_n is equal to the number of cycle types. This is the number of *partitions* of n. A partition of n is a way of writing n as a sum of positive integers. So for example the partitions of 4 are

$$4 = 1+1+1+1,\ 4 = 2+1+1,\ 4 = 2+2,\ 4 = 3+1,\ 4 = 4.$$

So there are 5 partitions of 4, meaning there are five conjugacy classes in S_4. The partition $1+1+1+1$ corresponds to the cycle type with four fixed points, which means the identity permutation. The partition $2+1+1$ corresponds to the cycle type with one cycle of length 2 and two fixed points, i.e. the transpositions (there are $\binom{4}{2} = 6$ of these in S_4). The partition 4 corresponds to the cycles of length 4, e.g. $(1\,2\,3\,4)$. There are 6 of these in S_4.

Unfortunately there is no neat formula that tells us how many partitions a given positive integer n has. For small values of n however, we can count them. Also, we can count the number of

elements in S_n with a given cycle type, so we can count the number of elements in each conjugacy class. Remember also that the number of elements in a conjugacy class of any group is the index of the centralizer of an element of that class. So we can also calculate the orders of the centralizer of an element of each class. This information is all given below for the example of S_5 - and S_6 is on Problem Sheet 3.

CONJUGACY CLASSES OF S_5

The order of S_5 is $5! = 120$.

1. Partition: 1+1+1+1+1
   Cycle type: 5 fixed points
   Representative of class: id
   No. of elements in class: 1
   Order of centralizer: 120

2. Partition: 2+1+1+1
   Cycle type: 1 2-cycle and 3 fixed points
   Representative of class: $(1\ 2)$
   No. of elements in class: $\binom{5}{2} = 10$
   Order of centralizer of an element of this class: $\frac{120}{10} = 12$

3. Partition: 2+2+1
   Cycle type: two disjoint 2-cycles and 1 fixed point
   Representative of class: $(1\ 2)(3\ 4)$
   No. of elements in class: $\binom{5}{2} \times \binom{3}{2} \times \frac{1}{2} = 15$
   Order of centralizer of an element of this class: $\frac{120}{10} = 12$

   Note on Count: We have $\binom{5}{2} = 10$ choices for the first transposition and having chosen this we have $\binom{3}{2} = 3$ choices for the second one. This would give $10 \times 3 = 30$ choices for a pair of disjoint transpositions written in a specified order. Since the order doesn't matter (i.e. $(1\ 2)(3\ 4)$ is the same permutation as $(3\ 4)(1\ 2)$, this estimate of 30 counts every pair of disjoint transpositions twice. We need to divide it by 2 to get the right number of elements with this cycle type.

4. Partition: 3+1+1
   Cycle type: one 3-cycle and 2 fixed points
   Representative of class: $(1\ 2\ 3)$
   No. of elements in class: $\binom{5}{3} \times \binom{2}{!} = 10 \times 2 = 20$
   Order of centralizer of an element of this class: $\frac{120}{20} = 6$

   Note on Count: We have $\binom{5}{3}$ choices for the three elements to put in our cycle. Having chosen them we have 2! ways to arrange them in cyclic order. For example if our three elements are 1,2,3, they can be arranged in cyclic order as $(1\ 2\ 3)$ or $(1\ 3\ 2)$.

5. Partition: 3+2
   Cycle type: one 3-cycle and one 2-cycle (disjoint from the 3-cycle)
   Representative of class: $(1\ 2\ 3)(4\ 5)$
   No. of elements in class: $\binom{5}{3} \times \binom{2}{!} = 10 \times 2 = 20$
   Order of centralizer of an element of this class: $\frac{120}{20} = 6$

   Note on Count: This is the same as the previous class, since having chosen the 3-cycle on one of 20 ways we have no choice about the 2-cycle.

6. Partition: 4+1
   Cycle type: one 4-cycle and one fixed point
   Representative of class: $(1\ 2\ 3\ 4)$
   No. of elements in class: $\binom{5}{4} \times \binom{3}{!} = 5 \times 6 = 30$
   Order of centralizer of an element of this class: $\frac{120}{30} = 4$

   Note on Count: We have $\binom{5}{4}$ choices for the four elements to be in our 4-cycle, and having chosen them there are 3! ways to arrange them in cyclic order. For example if our elements are 1,2,3,4 we can agree to write 1 first in our description of the cyclic order, we have 3 choices for what to put next, 2 after that and so on.

7. Partition: 5
   Cycle type: one 5-cycle
   Representative of class: $(1\ 2\ 3\ 4\ 5)$
   No. of elements in class: $4! = 24$
   Order of centralizer of an element of this class: $\frac{120}{24} = 5$

So the number of conjugacy classes of S_5 is 7. We should find that our numbers of elements in each add up to 120:

$$1 + 10 + 15 + 20 + 20 + 30 + 24 = 120.$$

Note: We have shown that the centre of S_n (for $n \geqslant 3$) is trivial, since the centre consists exactly of those elements that have only one element in their conjugacy class. Every cycle type except the one with n fixed points is represented by more than one element.

The symmetric groups are exceptional in that their conjugacy classes have a nice combinatorial description. This is not really typical of finite groups.

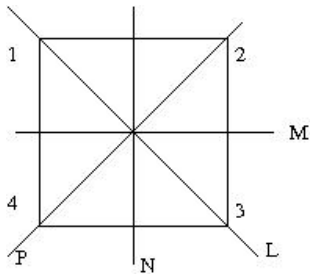
3.3 Cayley's Theorem

Cayley's Theorem tells us that every finite group of order n may be regarded as a subgroup of the symmetric group S_n. This is one of the reasons for the importance of the symmetric groups in group theory. To clarify what is meant by "may be regarded as", we need a definition.

Definition 3.3.1. *Two groups are said to be isomorphic to each other if after some relabelling of their elements they become exactly the same.*

For example, back in Chapter 1 we saw that the elements of the group D_6 of symmetries may be identified with permutations of the vertices. Every one of the six permutations of the three vertices arises this way - the two three cycles as the two rotations, the three transpositions as the three reflections, and the identity permutation as the identity symmetry obviously. Moreover, we saw that with this association, composition of symmetries corresponds exactly to multiplication of the associated permutations. We would say then that D_6 is *isomorphic* to S_3, the full group of permutations of three objects.

Similarly we can associate a permutation from S_4 to every symmetry of a square. Suppose that our square has vertices $1, 2, 3, 4$ as in the diagram below, and axes of symmetry L, M, N, P. Let S_L, S_M, S_N, S_P denote the reflections in these axes and let R_{90}, R_{180}, R_{270} denote the counter clockwise rotations through $90°$, $180°$ and $270°$.



Then the symmetries are associated to permutations in S_4 as follows.

$\mathrm{id} \leftrightarrow \mathrm{id}$	$S_M \leftrightarrow (1\,4)(2\,3)$
$R_{90} \leftrightarrow (1\,4\,3\,2)$	$S_N \leftrightarrow (1\,2)(3\,4)$
$R_{180} \leftrightarrow (2\,4)(1\,3)$	$S_L \leftrightarrow (2\,4)$
$R_{270} \leftrightarrow (1\,2\,3\,4)$	$S_P \leftrightarrow (1\,3)$

This establishes that D_8 is isomorphic to a subgroup of S_4. Note that this is not a subgroup of A_4, since the permutations involved are not all even (this is related to the last two problems on Problem Sheet 3).

The main goal of the rest of this section is to discuss Cayley's Theorem, which dates back to 1854, though not quite in its modern form. Cayley's Theorem shows that in a group of finite order n, we may associate to each element a permutation of the group elements, and hence establish an isomorphism between the group and some subgroup of S_n. Note that in the case of D_8, Cayley's Theorem would say that D_8 is isomorphic to some subgroup of S_8. This is not really connected to the above observation that D_8 is isomorphic to a subgroup of S_4, obtained by regarding its elements as permuations of four vertices.

The key ingredient in the proof of Cayley's theorem is the following connection between (general) group elements and permutations.

Let G be a group of order n, with elements $g_1 (= \mathrm{id}), g_2, g_3, \ldots, g_n$. Let $g \in G$ (so g is one of the g_i). Define a function ϕ_g from G to G by

$$\phi_g(g_i) = gg_i.$$

Note that each gg_i is an element of G, and that gg_i and gg_j are different whenever g_i and g_j are different. Thus ϕ_g is a permutation of the n elements of G. If you write out the group table for

G, then ϕ_g is the permutation of the elements of G that is written into the row corresponding to g. Thus each element of G can be associated to a particular permutation of the n elements of G, which may be regarded as an element of S_n. We have a correspondence

$$g \leftrightarrow \phi_g$$

between g and the set $\{\phi_g : g \in G\}$ of permutations.

Finally, for elements g and h of G, notice that for each g_i

$$\phi_g(\phi_h(g_i)) = \phi_g(hg_i) = g(hg_i) = ghg_i = \phi_{gh}(g_i).$$

Thus the composition of $\phi_g \circ \phi_h$ of the permutations corresponding to g and h is the permutation corresponding to the product gh in G. This means that the above correspondence between group elements and permutations is not only a correspondence of elements of G with elements of S_n, it is also a correspondence of the group operation of G with composition of permutations in S_n. Thus it establishes that G is isomorphic to a subgroup of S_n. We finish with the "official" statement of Cayley's Theorem.

Theorem 3.3.2 (Cayley, 1854)**.** *Let G be a group of order n. Then G is isomorphic to some subgroup of the symmetric group S_n.*

Chapter 4

Normal subgroups and quotient groups

4.1 Group Homomorphisms

Many areas of mathematics involve the study of functions between sets that are of interest. Generally we are not interested in *all* functions but only those that interact well with particular properties or themes - for example in calculus we are usually interested in continuous or maybe differentiable functions - these are the ones to which the principles of calculus apply. In linear algebra, we don't study all functions between vector spaces, we study the ones that preserve addition and multiplcation by scalars, and refer to these as *linear transformations*. Likewise in group theory, we are interested in functions between groups that preserve the group operations in the sense of the following definition.

Definition 4.1.1. *Let* G *and* H *be groups with operations* $\star_G$ *and* $\star_H$ *respectively. A function* $\phi : G \to H$ *is a* group homomorphism *if for all elements* x *and* y *of* G

$$\phi(x \star_G y) = \phi(x) \star_H \phi(y).$$

This is saying that $\phi : G \to H$ is a group homomorphism if for any pair of elements x and y of G, combining them in G and then applying ϕ always gives the same result as separately applying ϕ to the two of them and then combining their images using the group operation in H.

EXAMPLES OF GROUP HOMOMORPHISMS

1. **The Determinant**
   Let $\mathbb{Q}^\times$ denote the group of non-zero rational numbers under multiplication, and as usual let $GL(3, \mathbb{Q})$ denote the group of invertible 3×3 matrices with rational entries, under multiplication.

   The function $\det : GL(3, \mathbb{Q}) \to \mathbb{Q}^\times$ that sends every matrix to its determinant is a group homomorphism, since $\det(AB) = \det(A)\det(B)$ if A and B are 3×3 matrices with rational entries.

2. Let H denote the group $\{1, -1\}$ under multiplication (the 1 and -1 here are just the ordinary numbers 1 and -1, H is a group of order 2). For any natural number n, we may define a function $\phi_n : S_n \to H$ by
   $$\phi_n(\pi) = \begin{cases} 1 & \text{if } \pi \text{ is even} \\ -1 & \text{if } \pi \text{ is odd} \end{cases}$$
   Then ϕ_n is a group homomorphism for all n. To see this suppose that π_1 and π_2 are elements of S_n. There are four cases to check.

- If π_1 and π_2 are both even then so is $\pi_1\pi_2$ and

$$\phi_n(\pi_1)\phi_n(\pi_2) = 1 \times 1 = 1 = \phi_n(\pi_1\pi_2).$$

- If π_1 is even and π_2 is odd then $\pi_1\pi_2$ is odd and

$$\phi_n(\pi_1)\phi_n(\pi_2) = 1 \times (-1) = -1 = \phi_n(\pi_1\pi_2).$$

- If π_1 is odd and π_2 is even then $\pi_1\pi_2$ is odd and

$$\phi_n(\pi_1)\phi_n(\pi_2) = (-1) \times 1 = -1 = \phi_n(\pi_1\pi_2).$$

- If π_1 and π_2 are both odd then $\pi_1\pi_2$ is even and

$$\phi_n(\pi_1)\phi_n(\pi_2) = (-1) \times (-1) = 1 = \phi_n(\pi_1\pi_2).$$

3. The function τ from $\mathbb{Z}$ to $\mathbb{Z}$ defined for $a \in \mathbb{Z}$ by $\tau(a) = 3a$ is a homomorphism from the additive group $(\mathbb{Z}, +)$ to itself. To see this, note for $a, b \in \mathbb{Z}$ that

$$\tau(a + b) = 3(a + b) = 3a + 3b = \tau(a) + \tau(b).$$

Exercise: Show that the function f from $\mathbb{Z}$ to $\mathbb{Z}$ defined for $a \in \mathbb{Z}$ by $f(a) = a + 1$ is *not* a group homomorphism (from $(\mathbb{Z}, +)$ to itself).

If $\phi : G \to H$ *is* a group homomorphism, then there is a subgroup of G and a subgroup of H naturally associated with ϕ. These are defined below.

Definition 4.1.2. *Suppose that $\phi : G \to H$ is a homomorphism of groups. Then*

1. *The* kernel *of ϕ is the subset of G consisting of all those elements whose image under ϕ is id_H.*

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

2. *The* image *of ϕ is the subset of H consisting of all those elements that are the images under ϕ of elements of G.*

$$\mathrm{Im}\phi = \{h \in H : h = \phi(g) \text{ for some } g \in G\}.$$

It is fairly routine to prove that the kernel and image of ϕ are not only subsets but subgroups of G and H respectively. This is the content of the next two lemmas.

Lemma 4.1.3. *Suppose that $\phi : G \to H$ is a homomorphism of groups. Then* $\ker \phi$ *is a subgroup of* G.

Proof. First we show that $id_G \in \ker \phi$. Let $g \in G$ and let $h = \phi(g)$ in H. Then

$$h = \phi(g) = \phi(id_G \star_G g) = \phi_(id_G) \star_H \phi(g) = \phi(id_G) \star_H h.$$

Thus $\phi(id_G)$ is an element of H that satifies

$$h = \phi(id_G) \star_H h$$

for some element h of H. Multiplying both sides of the above equation on the right by h^{-1}, it follows that $\phi(id_G) = id_H$ and hence that $id_G \in \ker \phi$.

Now suppose that $g_1, g_2 \in \ker \phi$. Then

$$\phi(g_1 \star_G g_2) = \phi(g_1) \star_H \phi(g_2) = id_H \star_H id_H = id_H.$$

Hence $g_1 \star_G g_2 \in \ker \phi$ and $\ker \phi$ is closed uder the operation of G.

Finally let $g \in \ker \phi$. We need to show that $g^{-1} \in \ker \phi$ aswell. We know that $\phi(g) = id_H$ and (from above) that $\phi(id_G) = id_H$. Now

$$\begin{aligned} id_H &= \phi(id_G) \\ &= \phi(g \star_G g^{-1}) \\ &= \phi(g) \star_H \phi(g^{-1}) \\ &= id_H \star_H \phi(g^{-1}) \\ &= \phi(g^{-1}). \end{aligned}$$

Thus $g^{-1} \in \ker \phi$, as required. □

Remark: Note that the last part of the above proof shows that $\phi(g)$ and $\phi(g^{-1})$ are inverses of each other in H, for any element g of G.

Lemma 4.1.4. *Suppose that* $\phi : G \to H$ *is a homomorphism of groups. Then* $\mathrm{Im}\phi$ *is a subgroup of* H.

Proof. From the proof of Lemma 4.1.3 above we know that $\phi(id_G) = id_H$, so $id_H \in \mathrm{Im}\phi$.

Suppose that $h_1, h_2 \in \mathrm{Im}\phi$. Then $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some elements g_1 and g_2 of G. Then

$$\phi(g_1 \star_G g_2) = \phi(g_1) \star_H \phi(g_2) = h_1 \star_H h_2,$$

so $h_1 \star_H h_2 \in \mathrm{Im}\phi$ and $\mathrm{Im}\phi$ is closed under $\star_H$.

Finally suppose $h \in \mathrm{Im}\phi$. We need to show that $h^{-1} \in \mathrm{Im}\phi$ also. We know that $h = \phi(g)$ for some $g \in G$, and that

$$id_H = \phi(id_G) = \phi(g \star_G g^{-1}) = \phi(g) \star_H \phi(g^{-1}) = h \star_H \phi(g^{-1}).$$

Since $h \star_H \phi(g^1) = id_H$, it follows that $h^{-1} = \phi(g^{-1})$ and thus that $h^{-1} \in \mathrm{Im}\phi$. □

Examples

1. **The Determinant** The kernel of the function $\det : GL(3, \mathbb{Q}) \to \mathbb{Q}^\times$ that sends every matrix to its determinant is the subgroup consisting of all those matrices of determinant 1 in $GL(3, \mathbb{Q})$. This is denoted $SL(3, \mathbb{Q})$ and called the *special linear group* of 3×3 matrices over $\mathbb{Q}$.

   The image of det is the full group $\mathbb{Q}^\times$ of non-zero rational numbers, since every non-zero rational number arises as the determinant of some 3×3 matrix with rational entries.

2. Let $\phi_n : S_n \to \{1, -1\}$ be defined by by

$$\phi_n(\pi) = \begin{cases} 1 & \text{if } \pi \text{ is even} \\ -1 & \text{if } \pi \text{ is odd} \end{cases}$$

   Then the kernel of ϕ_n is A_n, the group of even permutations in S_n. The image of ϕ_n is $\{1, -1\}$.

3. The homomorphism τ from $(\mathbb{Z}, +)$ to $(\mathbb{Z}, +)$ defined for $a \in \mathbb{Z}$ by $\tau(a) = 3a$ has trivial kernel $\{0\}$, and its image is the subgroup of $(\mathbb{Z}, +)$ consisting of all multiples of 3.

4.2 Normal Subgroups

Suppose that $\phi : G \to H$ is a homomorphism of groups, and let N denote the kernel of ϕ. So N consists of all those elements x of G for which $\phi(x) = id_H$. In particular the elements of N all have the same image under ϕ.

Now let g be an element of G and suppose that $g \notin N$. Write h for the image of y under ϕ, so $h = \phi(y)$ and $h \neq id_H$ in H. Now consider the set of all elements of G whose image under ϕ is h. How is this related to y and to N?

- Let $n \in N$. Then $\phi(gn) = \phi(g)\phi(n) = hid_H = h$. This means that every element of the left coset gN of N in G has image h.
- On the other hand suppose that $\phi(g') = h$ for some $g' \in G$. Then $g' = g(g^{-1}g')$ and

$$h = \phi(g') = \phi(g)\phi(g^{-1}g') = h\phi(g^{-1}g').$$

  Since $h = h\phi(g^{-1}g')$, it follows that $\phi(g^{-1}g') \in N$ and hence that $g' \in gN$.

Thus, if $\phi(g) = h$, then the set of elements of G whose image under ϕ is h is exactly the left coset gN.

On the other hand, a very similar argument shows that the set of elements of G whose image under ϕ is h is exactly the *right coset* Ng.

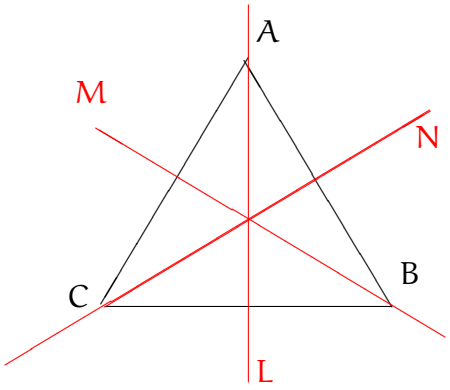
- If $n \in N$, then $\phi(ng) = \phi(n)\phi(g) = id_H h = h$.
- On the other hand if $\phi(g') = h$ for some $g' \in G$ then $g' = (g'g^{-1})g$ and $g'g^{-1} \in N$ since $\phi(g'g^{-1})h = h \implies \phi(g'g^{-1}) = id_H$. So g' belongs to the right coset Ng of N in G.

The conclusion from the above discussion is: if $\phi : G \to H$ is a group homomorphism with kernel N, and if $g \in G$, then the subset of G consisting of those elements whose image under ϕ is the same as that of g is equal to both the left coset gN and the right coset Ng. In particular, for every $g \in G$, the left coset gN and the right coset Ng are equal to each other as sets.

Definition 4.2.1. *Let* N *be a subgroup of a group* G. *If* $gN = Ng$ *for every* $g \in G$, *then* N *is said to be a* normal subgroup *of* G. *This situtaion is denoted* $N \trianglelefteq G$.

Examples of normal and non-normal subgroups

Consider the group D_6 of symmetries of the equilateral triangle, labelled id, $R_{120}, R_{240}, S_L, S_M, S_N$, with axes M, L, N as in the diagram below.



The table for D_6 is as follows.

	id	R_{120}	R_{240}	S_L	S_M	S_N
id	id	R_{120}	R_{240}	S_L	S_M	S_N
R_{120}	R_{120}	R_{240}	id	S_M	S_N	S_L
R_{240}	R_{240}	id	R_{120}	S_N	S_L	S_M
S_L	S_L	S_N	S_M	id	R_{240}	R_{120}
S_M	S_M	S_L	S_N	R_{120}	id	R_{240}
S_N	S_N	S_M	S_L	R_{240}	R_{120}	id

Let H denote the subgroup $\{id, S_L\}$ of order 2 of D_6. To determine whether H is a normal subgroup of D_6 or not, look at the left and right cosets of H in D_6 determined by each element. For example

$$S_N H = \{S_N \circ id, S_N \circ S_L\} = \{S_N, R_{240}\}.$$

On the other hand

$$HS_N = \{id \circ S_N, S_L \circ S_N\} = \{S_N, R_{120}\}.$$

Since the right and left cosets of H determined by the element S_N are different sets, we can say that H is *not* a normal subgroup of D_6.

Let T denote the subgroup of D_6 consisting of the three rotations id, R_{120} and R_{240}. For each element of D_6 we can investigate whether the left and right cosets of N that they determine coincide or not.

- In the case of the elements id, R_{120} and R_{240} of N, the left and right cosets of T that these determine are all equal to T itself and in particular all equal to each other.
- The left coset of T determined by S_L is

  $$\{S_L \circ id, S_L \circ R_{120}, S_L \circ R_{240}\} = \{S_L, S_N, S_M\}.$$

  The right coset of T determined by S_L is

  $$\{id \circ §_L, R_{120} \circ S_L, R_{240} \circ S_L\} = \{S_L, S_M, S_N\}.$$

  Thus $S_L T = TS_L$.
  You can check that it is also true for the other two reflections that $S_M T = TS_M$ and $S_N T = TS_N$. Having checked all of these we can state that T is a *normal subgroup* of D_6.

Other characterizations of normality

Our "official" definition of normality is that a subgroup N of a group G is *normal* in G if and only if for every $g \in G$, the left coset gN is equal to the right coset Ng. This does not have to means that $gn = ng$ for all $g \in G$ and for all $n \in N$ (although that is a possibility that arises if N is in the centre of G). Note that

- In an abelian group, all subgroups are normal.
- In any group G, all subgroups of the centre $Z(G)$ are normal in G.

Suppose that N is a normal subgroup of a group G. This means that for every $g \in G$, every element of the left coset gN also belongs to the right coset Ng. This means that for all $g \in G$ and all $n \in N$,

$$gn = n'g$$

for some $n' \in N$. Multiplying the above equation (on the right) by g^{-1}, this means that

$$gng^{-1} \in N, \ \forall g \in G, \text{ and } \forall n \in N.$$

This is saying that a normal subgroup must be closed under conjugation in the whole group: *if* N *is a normal subgroup of* G *and* $n \in N$*, then all conjugates of* n *in* G *belong to* N.

On the other hand, if a subgroup of G has the above property, then it *is* normal, as the following Lemma shows.

Lemma 4.2.2. *Let* N *be a subgroup of* G *with the property that* $gng^{-1} \in N$ *for all* $g \in G$ *and for all* $n \in N$. *Then* $gN = Ng$ *for all* $g \in G$, *so* $N \trianglelefteq G$.

Proof. Let $g \in G$. To show that $gN \subseteq Ng$, let gn be a typical element of the left coset gN (so $n \in N$). Then $gng^{-1} = n'$ for some $n' \in N$, and $gn = n'g$ which means that gn belongs to the right coset Ng. Thus $gN \subseteq Ng$.

On the other hand let ng be a typcial element of the right coset Ng (so $n \in N$). Note that $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$, so $g^{-1}ng = n''$ for some $n'' \in N$. Then $ng = gn''$, so ng belongs to the left coset gN. Hence $Ng \subseteq gN$, and we conclude that $gN = Ng$ for all $g \in G$, which means that N is normal in G. □

The following (which are just alternative wordings of the same statement) are useful characterizations of normal subgroups that are equivalent to our original definition.

1. A subgroup N of a group G is *normal* in G if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.
2. A subgroup N of G is *normal* in G if N is closed under conjugation in G.
3. A subgroup N of G is *normal* in G if N is a union of conjugacy classes of G (and is a subgroup of course).

Looking back at our examples from D_6, we can interpret them in the context of the above statements.
We noted that the group $N = \{id, R_{120}, R_{240}\}$ of rotations *is* a normal subgroup of G; this is the union of the conjugacy classes $\{id\}$ and $\{R_{120}, R_{240}\}$.
We noted that the subgroup $H = \{id, S_L\}$ is *not* normal in D_6. We can explain this now by observing that this subgroup contains S_L but does not contain the elements S_M and S_N which are conjugate to S_L in D_6 - thus H is not closed under conjugation in D_6.

Example 4.2.3. *Using our knowledge from Chapter 3 we can see that the alternating group* A_n *is a normal subgroup of the symmetric group* S_n, *since it is the union of those conjugacy classes that consist of even permutations.*

We finish this section by noting that with our new understanding of normality in terms of conjugacy, it is easy to show that the kernel of a group homomorphism must be a normal subgroup.

Lemma 4.2.4. *Let* $\phi : G \to H$ *be a group homomorphism with kernel* N. *Then* N *is a normal subgroup of* G.

Proof. We know from Lemma 4.1.3 that N is a subgroup of G. To see that it is normal, let $n \in N$ and $g \in G$. We need to show that $gng^{-1} \in N$, which means that $\phi(gng^{-1}) = id_H$. We can see this as follows

$$\begin{aligned}
\phi(gng^{-1}) &= \phi(g)\phi(n)\phi(g^{1}) \\
&= \phi(g)\, id_H\, \phi(g^{1}) \\
&= \phi(g)\phi(g^{-1}) \\
&= \phi(gg^{-1}) \\
&= \phi(id_G) \\
&= id_H.
\end{aligned}$$

Thus $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$, and $N \trianglelefteq G$.

□

4.3 Quotient Groups

Let N be a normal subgroup of the group G. The theme of this section is to define a group structure on the set of left (or right) cosets of N in G, which is denoted by G/N.

To motivate this definition we give a relatively familiar example.

Example 4.3.1. *(Addition modulo 5)*

Let $5\mathbb{Z}$ denote the subgroup of $(\mathbb{Z}, +)$ consisting of all multiples of 5.

$$5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}.$$

There are five distinct cosets of $5\mathbb{Z}$ in $\mathbb{Z}$, as follows:

$$\begin{aligned} 5\mathbb{Z} &= \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}; \\ 1 + 5\mathbb{Z} &= \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\}; \\ 2 + 5\mathbb{Z} &= \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}; \\ 3 + 5\mathbb{Z} &= \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}; \\ 4 + 5\mathbb{Z} &= \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}. \end{aligned}$$

Note that $5 + 5\mathbb{Z} = 5\mathbb{Z}$, $6 + 5\mathbb{Z} = 1 + 5\mathbb{Z} = 11 + 5\mathbb{Z}$, etc. We give the names $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$ to the five cosets above, write $\mathbb{Z}/5\mathbb{Z}$ for the set consisting of these cosets, and define addition in $\mathbb{Z}/5\mathbb{Z}$ as in the following example:
To add $\bar{3}$ and $\bar{4}$, we choose a representative from each of these cosets, add the representatives in $\mathbb{Z}$, and then take the coset to which the result belongs. For example we could take 3 and 4 as our representatives, add them together to get 7, notice that 7 belongs to the coset $\bar{2}$ and conclude that $\bar{3} + \bar{4} = \bar{2}$.
Alternatively we could take 8 and -11 as our representatives of $\bar{3}$ and $\bar{4}$, adding these in $\mathbb{Z}$ would give -3 which again belongs to $\bar{2}$, so again we would conclude $\bar{3} + \bar{4} = \bar{2}$.
The key point is that the choice of representatives does not determine the outcome, and this is because $5\mathbb{Z}$ is a normal *subgroup of $\mathbb{Z}$.*

Let G be a group and let N be a normal subgroup of G. Let G/N (read this as "G mod N") denote the set of (left or right) cosets of N in G. Define an operation $\star$ on G/N by

$$xN \star yN = xyN,$$

where $x, y \in G$. This is basically saying that to "multiply" two cosets of N in G, we should take an element from each one, multiply them in G and then take the coset determined by the result.

We need to show that the operation $\star$ is well-defined in the following sense: if x, x_1, y, y_2 are elements of G for which $xN = x_1N$ and $yN = y_1N$, then we want to know that $xN \star yN = x_1N \star y_1N$, i.e. that $xyN = x_1y_1N$.

- Since $xN = x_1N$ we know that $xx_1^{-1} \in N$; write $xx_1^{-1} = n_x$.
- Since $yN = y_1N$ we know that $yy_1^{-1} \in N$: write $yy_1^{-1} = n_y$.
- What we need to do in order to show that $xyN = x_1y_1N$ is show that $xy(x_1y_1)^{-1} \in N$, i.e. that $xyy_1^{-1}x_1^{-1} \in N$. Now $xyy_1^{-1}x_1^{-1} = xn_yx_1^{-1}$. Now xn_y is in the left coset xN. Then it is in the right coset Nx, because N is normal in G. Then $xn_y = nx$ for some $n \in N$ and

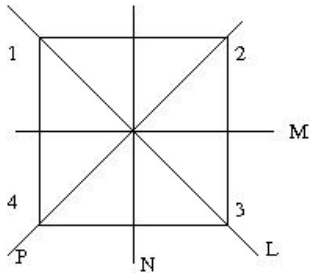
  $$xy(x_1y_1)^1 = xn_yx_1^{-1} = nxx_1^{-1} = nn_x \in N.$$

  This means that $xyN = x_1y_1N$, as required.

Now $\star$ defines a binary operation on G/N, the set of cosets of N in G. The coset N itself is an identity element for this operation. The operation $\star$ is associative because it is based on the associative operation of G. The inverse of the coset gN under $\star$ is the coset $g^{-1}N$. Thus G/N becomes a group under $\star$, called the *quotient group* G mod N.

Note: If G is finite, then the order of G/N is $[G : N] = \dfrac{|G|}{|N|}$.

Example 4.3.2. *Suppose that* D_8 *is the group of symmetries of the square (with axes as in the diagram below) and that* N *is the subgroup* $\{id, R_{180}\}$.



Then N *is a normal subgroup of* D_8 *and it has four cosets:*

$$N = \{id, R_{180}\},\ R_{90}N = \{R_{90}, R_{270}\},\ S_LN = \{S_L, S_P\},\ S_MN = \{S_M, S_N\}.$$

The multiplication table for the quotient group D_8/N *is as follows.*

	N	$R_{90}N$	S_LN	S_MN
N	N	$R_{90}N$	S_LN	S_MN
$R_{90}N$	$R_{90}N$	N	S_MN	S_LN
S_LN	S_LN	S_MN	N	$R_{90}N$
S_MN	S_MN	S_LN	$R_{90}N$	N