MATH08064 Fundamentals of Pure Mathematics

LECTURES

ON

GROUP THEORY

notes by Michael Wemyss

2015/16

Dr. Sue Sierra
JCMB 5606
s.sierra@ed.ac.uk

- The course follows closely the book
  [J] *Groups* by Jordan and Jordan (the library entry is here).
  The purpose of these notes is to record the lecture material, mainly to save you having to frantically write everything down during lectures, and to supplement the material contained in [J]. They are fully hyperlinked.

- References to the above book in these notes will be abbreviated by [J]; for example [J, §1.2] refers to section 1.2, whilst [J, Ex.7.4] refers to Exercise 4 in Section 7. When revision of first year topics is required, your first year books
  [L] *A Concise Introduction to Pure Mathematics* (third edition) by Liebeck
  [P] *Linear Algebra: A Modern Introduction* (third edition) by Poole
  will be referenced.

- Throughout the semester, all course information (including exercise sheets, workshop sheets and problems for handin) will be available on the course LEARN page, in the "Algebra" directory.

- Instructions for logging in to TopHat to answer the clicker–style questions are linked on the main course LEARN page. The direct weblink to login is
  https://app.tophat.com/
  and the course join code is 065339.

Contents

0. Revision

We need the following first year material, and will use it extensively throughout. We will revise other first year material as we require it.

0.1. **Functions**

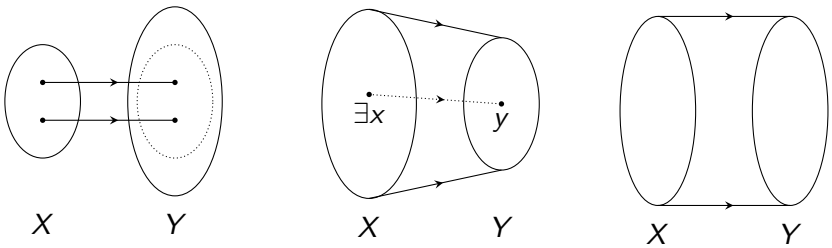
We need everything in [L, §19], so you are strongly recommended to review this material. It is also contained in [J, §2.2]. As notation, in this course we will write a function f from X to Y as $f : X \to Y$. Further, we will write the composition of functions $f : X \to Y$ and $g : Y \to Z$ as $g \circ f$, so $g \circ f$ means 'do f first, then g'.

0.1.1. *Definition.* A function $f : X \to Y$ is called

- *injective* if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$ (equivalently, if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$).
- *surjective* if for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$.
- *bijective* if it is both injective and surjective.

If f is bijective, we denote its inverse function by f^{-1}.

An easy way to remember this is via the pictures



injective
'don't lose information'

surjective
'hit everything'

bijective
'the same'

One key property of functions is that

$$(h \circ g) \circ f = h \circ (g \circ f).$$

This is easy to verify; see for example [J, p15].

1. Groups and Symmetries

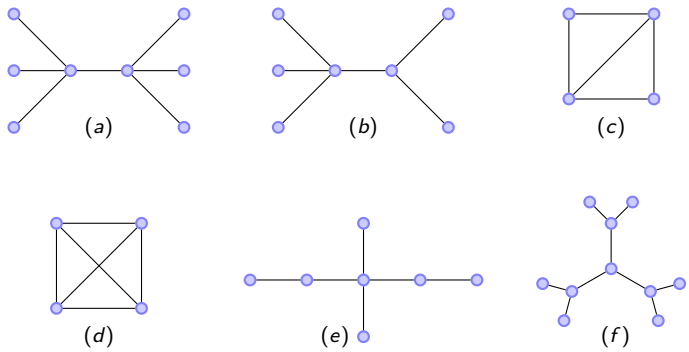
You are advised to read [J, §1]. Beware that it is an introductory chapter and so many things will only fully make sense later! The theme of [J, §1], and the first few lectures, is the slogan 'symmetries give groups'.

1.1. Symmetries of graphs

This section is a little more general than [J, §1.1], and will generate us many, many examples.

1.1.1. *Definition.* (similar to [L, §9]). A *graph* is a finite set of vertices joined by edges. We will assume that there is at most one edge joining two given vertices and no edge joins a vertex to itself. The *valency* of a vertex is the number of edges emerging from it.

1.1.2. *Examples.* The following are graphs.



The following are not graphs.

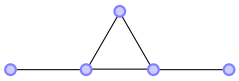
1.1.3. *Definition.* A *symmetry* of a graph is a permutation of the vertices that preserves the edges. More precisely, let V denote the set of vertices of a graph. Then a symmetry is a bijection $f : V \to V$ such that $f(v_1)$ and $f(v_2)$ are joined by an edge if and only if v_1 and v_2 are joined by an edge.

1.1.4. *Remarks.*

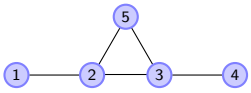
1. The mathematical definition of symmetry is independent of how we draw the graph. Thus you *must* use the mathematical definition, and not just rely on your intuition.

2. A symmetry $f\colon V \to V$ must preserve the valency of a vertex (prove this!). Hence if v_1 has valency three, then $f(v_1)$ must also have valency three.

1.1.5. *Example.* Describe all symmetries of the graph



For convenience, number the vertices

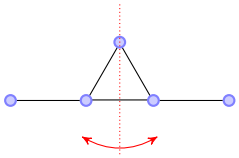


so V, the set of vertices, is $V = \{1, 2, 3, 4, 5\}$.

Let $f : V \to V$ be a symmetry of the graph. Since 5 is the only vertex with valency two, and symmetries preserve valencies, $f(5) = 5$. Since 2 and 3 are the only vertices that have valency three, either they are fixed ($f(2) = 2$ and $f(3) = 3$), or they are swapped ($f(2) = 3$ and $f(3) = 2$).

Case 1. Suppose that they are fixed. Thus by above 2, 3 and 5 are all fixed by f. Now $f(1)$ must be connected to $f(2) = 2$ and also have valency one, hence $f(1) = 1$. Similarly $f(4) = 4$. This means that f is the identity.

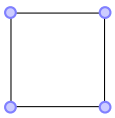
Case 2. Suppose that they are swapped. Thus by above we know $f(5) = 5$, $f(2) = 3$ and $f(3) = 2$. Now $f(1)$ must be connected to $f(2) = 3$ and have valency one, so $f(1) = 4$. Similarly $f(4) = 1$, so f is the symmetry



Thus there are precisely two symmetries of the graph, namely the identity and the above reflection.

1.1.6. *Logic.* When faced with a graph, it is often easy to guess some symmetries. However, when you want to determine *all* symmetries, you must argue that there are no more. This is usually more difficult. For example, in §1.1.5 we took an *arbitrary* symmetry and argued that it must be one of two things. This shows there are *precisely* two symmetries.

1.1.7. *Example.* In class we will determine the number of symmetries of the square



and we will draw what they are. The argument is quite brutal, and we will improve it a lot later. See also §1.3.

1.2. **Groups and Examples**

1.2.1. *Definition.* [J, §4.2] Let S be any nonempty set. An operation $*$ on S is a rule which, for every ordered pair (a, b) of elements of S, determines a unique element $a * b$ of S. Equivalently, if we recall that

$$S \times S := \{(a, b) \mid a, b \in S\},$$

then an operation is a function $S \times S \to S$.

1.2.2. *Example.* For any graph, we can consider the set

$$\mathcal{S} := \{\text{symmetries of that graph}\}.$$

The key point is that we can compose two symmetries f and g to obtain another symmetry (see the proof of G1 in §1.2.4 below). Thus we define $*$ by the rule $f * g := f \circ g$ (composition of functions), then this gives an operation on $\mathcal{S}$.

1.2.3. *Definition.* **(Definition of a Group)** [J, §4.3] We say that a nonempty set G is *group under* $*$ if

- G1. (Closure) $*$ is an operation, so $g * h \in G$ for all $g, h \in G$.
- G2. (Associativity) $g * (h * k) = (g * h) * k$ for all $g, h, k \in G$.
- G3. (Identity) There exists an *identity element* $e \in G$ such $e * g = g * e = g$ for all $g \in G$.
- G4. (Inverses) Every element $g \in G$ has an *inverse* g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Further, if G is a group, the number of elements in G is written $|G|$, and is called the *order* of G.

Groups are one of the basic building blocks of pure mathematics. One of the main reasons they are so important is that they appear often, and in many different contexts.

1.2.4. *Theorem.* The symmetries of a graph forms a group (under composition).

Proof. Let $f : V \to V$ and $g : V \to V$, then define $f * g$ to be their composition (as maps), so $f * g := f \circ g$, i.e. *do g first, then f.*

G1 The composition of two symmetries f and g is a symmetry, since
  (a) f, g are bijections implies that $f \circ g$ is a bijection.
  (b) v_1 and v_2 are joined by an edge if and only if $g(v_1)$ and $g(v_2)$ are joined by an edge if and only if $fg(v_1)$ and $fg(v_2)$ are joined by an edge.

  This shows that $f * g$ is a symmetry, so $*$ is an operation.

G2. The composition of maps is associative

$$(f * g) * h := (f \circ g) \circ h = f \circ (g \circ h) := f * (g * h)$$

  for all symmetries f, g, h (see §0).

G3. The identity map e which sends every vertex to itself is a symmetry, and obviously $e \circ f = f \circ e = f$ for all symmetries f.

G4. If $f : V \to V$ is a symmetry then it is bijective, so its inverse f^{-1} exists. It is also a symmetry (check!), and is characterized by $f \circ f^{-1} = f^{-1} \circ f = e$ (see [J, §2.2 Thm 1]).

Since axioms G1–G4 hold, the symmetries of a graph form a group. □

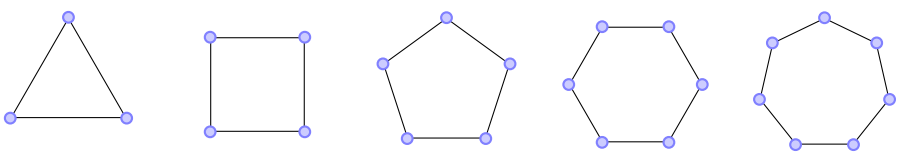
1.2.5. *Notation.* In the definition of a group, since associativity holds we usually drop brackets and write $g * h * k$ instead of $g * (h * k)$ or $(g * h) * k$.

1.2.6. *More examples.* Groups unify many things that you already know. I claim that you already know lots of examples of groups.

1. The integers $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ is a group under the operation $g * h := g + h$. Just check the axioms — if g and h are integers, so is $g + h$ and so the operation is closed. Adding integers is associative. The identity is 0 (since $0 + g = g + 0 = 0$ for all $g \in \mathbb{Z}$) and the inverse of g is $-g$ (since $g + (-g) = (-g) + g = e$ for all $g \in \mathbb{Z}$).
2. Similarly $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ (or indeed any other field) are all groups under addition.
3. [L, p109] For all $n \in \mathbb{N}$, the *integers mod n*, $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$, forms a group under addition. Again the identity is 0, and the inverse of x is $-x$ (taken mod n).
4. [P, §6] Every vector space V is a group under addition of vectors, with identity the zero vector. When we think of a vector space in this way we are forgetting the extra structure of scalar multiplication that a vector space has.
5. $M_n(\mathbb{R}) = \{n \times n$ matrices with coefficients in $\mathbb{R}\}$ is a group under addition.
6. The non-zero real numbers $\mathbb{R}^*$ form a group under multiplication (by which we mean $x * y := xy$) with identity 1 and the inverse of x being $1/x$. Similarly the non-zero elements of any field form a group under multiplication. For example, the non-zero elements $\mathbb{Z}_p^*$ (where p is prime) of $\mathbb{Z}_p$ form a group under multiplication, with identity 1 and inverse $1/x$.

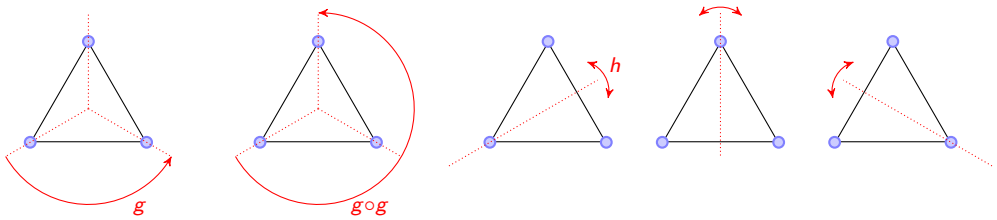
1.3. Symmetries of regular n-gons (=dihedral groups)

We view the n-gon as a graph, and apply the last section. In particular, by §1.2.4 the symmetries of an n-gon form a group. Here we investigate these in more detail.



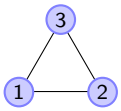
$n = 3$ $n = 4$ $n = 5$ $n = 6$ $n = 7$

1.3.1. *Symmetries of an equilateral triangle.* Consider a 3-gon, i.e. an equilateral triangle. There are precisely six symmetries of the 3-gon:

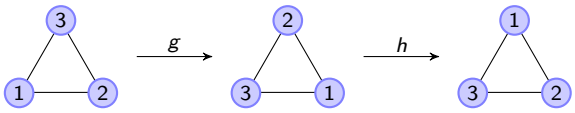


- e the identity (not drawn above).
- Rotation anticlockwise by $2\pi/3$ (which we call g), and rotation anticlockwise by $4\pi/3$. The latter is drawn in the second diagram, and corresponds to performing g twice.
- The three reflections in the lines through the three vertices. These are drawn in the last three diagrams.

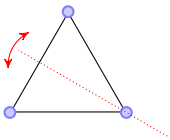
The proof that these six symmetries are all the symmetries of the 3-gon is rather similar to the proof in §1.1.5 (see Problem 1.3). Now if we label the vertices as



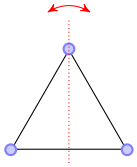
then



and so $h \circ g$ ($=g$ first then h) is equal to



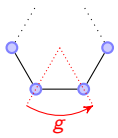
Similarly $g \circ h$ is equal to



and so $D_3 = \{e, g, g \circ g, h, g \circ h, h \circ g\}$. As a piece of notation we usually drop the symbol $\circ$ and so $D_3 = \{e, g, g^2, h, gh, hg\}$. See also Problem 1.3.

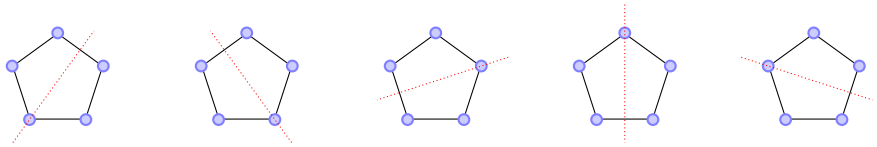
1.3.2. *The dihedral group.* Consider now a regular n-gon (where $n \geq 3$). Its symmetry group is called the *dihedral group* D_n. It has precisely $2n$ elements, namely:

- The identity e.
- The $n-1$ rotations through angles $k2\pi/n$ ($k = 1, \ldots, n-1$) anticlockwise. If we denote g to be the rotation anticlockwise through $2\pi/n$, i.e.

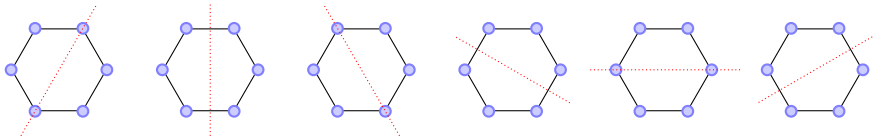


then the rotations are $\{g, g^2, \dots, g^{n-1}\}$.

- The n reflections. Pictorially the reflections depend on whether n is even or odd. For example when $n = 5$, there are five reflections which all take place in lines through vertices

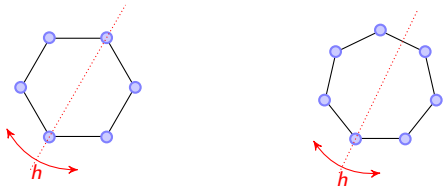


whereas if $n = 6$ there are six reflections



where some lines don't pass through any vertices. Regardless of whether n is even or odd, there are n reflections.

If we denote h to be the reflection in the line through the bottom left vertex, i.e.



n even $\qquad$ n odd

then $D_n = \{e, g, g^2, \dots, g^{n-1}, h, gh, g^2h, \dots, g^{n-1}h\}$. You should check this by doing Problem 1.4.

1.4. **Symmetries of finite sets (=the symmetric group)**

You encountered permutations in [L, §20] and you are strongly recommended to review the material there. Below summarizes [J, §2].

1.4.1. *Symmetric groups.* A symmetry of a set X of n objects is a *permutation* (i.e. a bijection $X \to X$). The set of all symmetries of X is denoted S_n. It has precisely $n!$ elements.

1.4.2. *Notes.*

1. The set S_n is a group under composition — we call it the *symmetric group*.

   Proof. We can view S_n as the set of symmetries of the graph

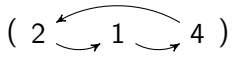
   where there are n vertices an no edges. Thus S_n is a group by 1.2.4. □

2. We usually label the elements of X by numbers, so $X = \{1, 2, \dots, n\}$. Thus to give a bijection $X \to X$, we have to specify where every number gets sent. Recall from [L, §20] that there are two ways of doing this.

The first method is '2-row array' notation where an element $f \in S_n$ is specified by the 2-row array

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

We also have cycle notation; revise [L, §20]. In this notation, (214) means the permutation where $2 \mapsto 1$, $1 \mapsto 4$, $4 \mapsto 2$, and all the other elements are fixed. You should read (214) as "2 goes to 1 goes to 4 goes to 2" and visually think of it as



(but don't write the arrows, just write (214)). Since all the other elements are by definition fixed, for example $(214) \in S_5$ corresponds to

$$(214) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$

in the 2-row array notation.

3. Although D_3 and S_3 have different definitions it turns out (see §4.1.4) that they are really "the same" group. The technical term is *isomorphic* — we will give a more precise definition later.

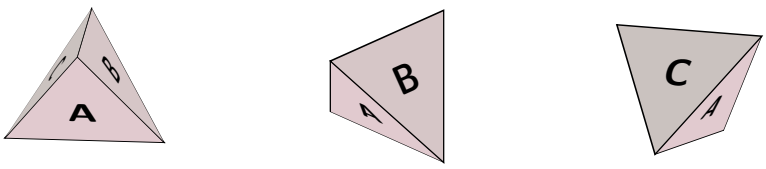
We will come back to symmetric groups later in §6.

1.5. (Rotational) Symmetries of regular solids

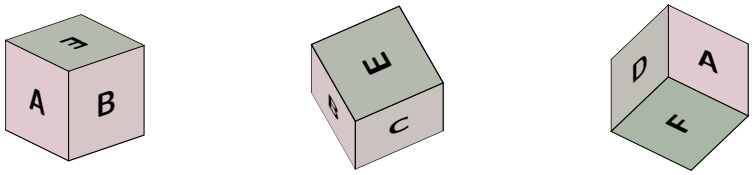
Recall [L, p77–78] that there are five platonic solids "fire, earth, air, ether and water", convex bodies whose faces are all the same regular n-gon, where every vertex is identical. They are:

	Faces	Edges	Vertices	Faces per vertex
tetrahedron	4 triangles	6	4	3
hexahedron	6 squares	12	8	3
octahedron	8 triangles	12	6	4
dodecahedron	12 pentagons	30	20	3
icosahedron	20 triangles	30	12	5

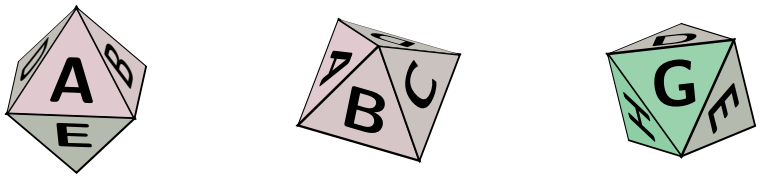
The tetrahedron:



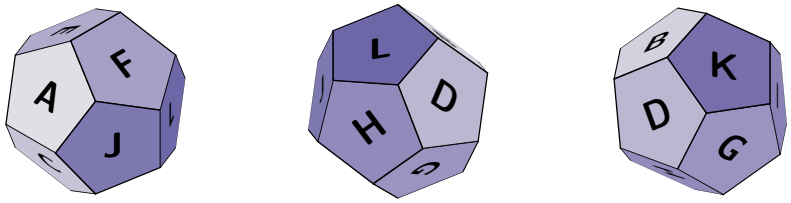
The hexahedron(=the cube):



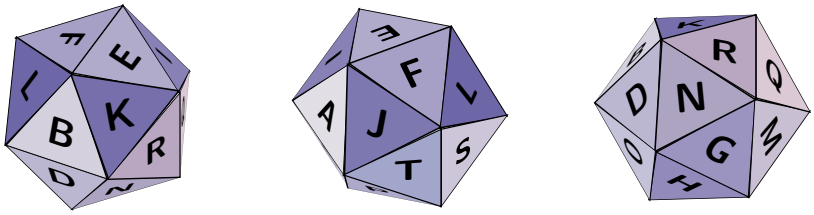
The octahedron:



The dodecahedron:



The icosahedron:



In this course we will consider their groups of *rotational symmetries*, namely those rotations (necessarily about the centres of faces, vertices and edges) that leave the solid fixed.

The Platonic solids have interesting symmetries, but it is much harder to prove anything about them (e.g. how many rotational symmetries there are) by arguing directly as in §1.1. We will come back to these examples in §6 after we know some more theory. In the meantime, you can construct your very own dodecahedron 2016 calendar at

http://www.maths.ed.ac.uk/∼ssierra/Calendar2016.pdf.

1.6. **Symmetries of vector spaces**

Recall from linear algebra that if $A, B \in M_n(\mathbb{R})$ then

1. A is invertible if and only if $\det A \neq 0$.
2. If A and B are invertible, so is AB, and further $(AB)^{-1} = B^{-1}A^{-1}$.

The first can be found in [P, Remark on p285], the second in [P, Thm 3.9 p173].

1.6.1. *Definition.* The set of *invertible* $n \times n$ matrices with coefficients in $\mathbb{R}$ is denoted $\mathrm{GL}(n, \mathbb{R})$. Similarly, if p is a prime, then the set of invertible $n \times n$ matrices with coefficients in $\mathbb{Z}_p$ is denoted $\mathrm{GL}(n, \mathbb{Z}_p)$.

1.6.2. *Theorem.* $\mathrm{GL}(n, \mathbb{R})$ is a group under matrix multiplication.

Proof. With $A * B := AB$ (matrix multiplication), we check the axioms:

G1. Closure follows from property 2 above.
G2. Associativity is [P, p229].
G3. The identity matrix is clearly the identity element.
G4. The inverse matrix gives the inverse element (by definition, see [P, p169]).

□

Similarly, when p is a prime, $\mathrm{GL}(n, \mathbb{Z}_p)$ is a group under matrix multiplication.

2. First Properties of Groups

This section covers [JJ, §4–§6]. From now on we assume only the group axioms.

2.1. First basic properties

2.1.1. *Lemma.* Let G be a group. If $g, h \in G$, then

1. There is one and only one element $k \in G$ such that $k * g = h$.
2. There is one and only one element $k \in G$ such that $g * k = h$.

Proof. 1. Let $k := h * g^{-1}$. Then

$$k * g = (h * g^{-1}) * g = h * (g^{-1} * g) = h * e = h,$$

which proves existence. Now suppose that $k' * g = h$. Then

$$k = h * g^{-1} = (k' * g) * g^{-1} = k' * (g * g^{-1}) = k' * e = k'$$

and so k is unique.
2. is very similar (check!). □

2.1.2. *Remark.* Note how every equality in the above proof is either an appeal to something we have already defined, or is justified by one of the axioms.

2.1.3. *Corollaries.* (see also [J, §4.5])

1. In a group you can always cancel: if $g * s = g * t$ then $s = t$. Similarly, if $s * g = t * g$ then $s = t$.
2. Inverses are unique: given $g \in G$ then there is one and only one element $h \in G$ such that $g * h = e$. In particular, $e^{-1} = e$ and $(g^{-1})^{-1} = g$.
3. A group has only one identity: if $g * h = h$ (even just for one particular h) then $g = e$.

Proof. 1. Let $h := g * s$. Then also $h = g * t$, so by uniqueness in §2.1.1, $s = t$.
2. The first statement is immediate from §2.1.1. Since $e * e = e$ (by group axiom 3) and $e * (e^{-1}) = e$ (by group axiom 4), the second statement follows from the first. Also, since $g^{-1} * (g^{-1})^{-1} = e$ and $(g^{-1}) * g = e$, it follows that $(g^{-1})^{-1} = g$.
3. We have $g * h = h = e * h$, so by cancelling h on the right (using part 1), $g = e$. □

2.2. Commutativity

2.2.1. *Definition.* Suppose that G is a group and $g, h \in G$. If $g * h = h * g$ then we say that g and h *commute*. If $g * h = h * g$ for all $g, h \in G$, then we say G is an *abelian* group.

2.2.2. *Remark.* It is very important to remember that not all groups are abelian.

2.2.3. *Examples and Non-examples.*

1. $\mathbb{R}$, $\mathbb{R}^n$, ... vector spaces are abelian groups under addition.
2. $\mathbb{Z}_n$ (the integers mod n) is an abelian group.
3. $\mathrm{GL}(2,\mathbb{R})$ is not an abelian group.
4. D_3 is not an abelian group, since $g \circ h \neq h \circ g$ (where g and h are defined in §1.3.1).

2.3. **Products**

The easiest way of making a new group out of given ones.

2.3.1. *Theorem.* Let G, H be groups. The product $G \times H = \{(g,h) \mid g \in G, h \in H\}$ has the natural structure of a group as follows:

- The group operation is $(g,h) * (g',h') := (g *_G g', h *_H h')$ (where we write $*_G$ for the group operation in G, etc).
- The identity e in $G \times H$ is $e := (e_G, e_H)$ (where we write e_G for the identity in G, etc).
- The inverse of (g,h) is (g^{-1}, h^{-1}) (the inverse of g is taken in G, and the inverse of h is taken in H).

We will usually drop the subscripts from the notation.

Proof. We need to check the axioms to ensure that $G \times H$ is a group. This is a good exercise, or see [J, §4.6]. □

2.3.2. *Notation.* Whenever G and H are groups, we will always regard $G \times H$ as a group under the operation defined above.

2.3.3. *Note.* If G, H are both finite then

$$|G \times H| = |G|\,|H|\,.$$

2.3.4. *Examples.*

1. You already know examples of products. Let $\mathbb{R}$ be regarded as an abelian group under addition. Then the vector space $\mathbb{R}^2$, regarded as a group under addition, is just $\mathbb{R} \times \mathbb{R}$ defined above.
2. Consider the graph (e) in §1.1.2. Its symmetry group is $S_2 \times S_2$, since any symmetry is given by specifying a permutation of the up–down arms, and a permutation of the left–right arms, i.e. a pair of permutations. For a more rigorous proof, see §4.2.6 later.

We will come back to products in §4.2.

2.4. **Subgroups**

2.4.1. *Definition.* [J, §5] Let G be a group. We say that a nonempty subset H of G is a *subgroup* of G if H itself is a group (under the operation from G). We write

$H \leq G$ if H is a subgroup of G. If also $H \neq G$, we write $H < G$ and say that H is a proper subgroup.

2.4.2. *Lemma.* Suppose that $H \leq G$. Then

1. $e_H = e_G$
2. If $h \in H$, the inverse of h in H equals the inverse of h in G.

Proof. 1. $e_H * e_H = e_H$ by the identity axiom in H and $e_G * e_H = e_H$ by the identity axiom in G. Hence $e_H * e_H = e_G * e_H$ so by cancellation $e_H = e_G$.
2. Let a denote the inverse of h in H, so $a*h = h*a = e_H$. By part 1, $a*h = h*a = e_G$ so a is also the inverse of h in G. □

2.4.3. *Theorem.* (Test for a subgroup) $H \subseteq G$ is a subgroup of G if and only if

S1. H is not empty.
S2. If $h, k \in H$ then $h * k \in H$
S3. If $h \in H$ then $h^{-1} \in H$.

Proof. ($\Leftarrow$) Suppose that H satisfies conditions S1, S2 and S3. We check the axioms of a group.

G1 By S2, H is closed under the operation $*$.
G2 Associativity holds in H since it holds in G.
G3 By S1 there exists $h \in H$. By S3 there exists $h^{-1} \in H$. By S2 $h * h^{-1} \in H$. hence $e_G \in H$. It acts as the identity for elements in H since it does so for all elements in G.
G4 Inverses exist in H by S3.

($\Rightarrow$) Suppose H is a subgroup of G, i.e. H is a group in its own right. Then by definition H is non-empty (so S1 holds), is closed (hence S2) and has inverses (hence S3). □

2.4.4. *Note.* If G is finite, then there is a slightly easier test for a subgroup. See Problem 2.2.

2.4.5. *Examples.* The test for a subgroup can be used to establish all the following examples.

1. G is a subgroup of itself. Also, $\{e\}$ is a subgroup of G, called the *trivial subgroup*.
2. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ (all abelian groups under addition).
3. Consider $G = S_3$. Let H denote all the permutations that send 1 to itself. (There are two of them, the identity and the one that swaps 2 and 3.) Then $H < G$.
4. Let $G = \mathbb{Z}_8$ (under addition) and let $H = \{0, 2, 4, 6\}$. Then $H < G$.
5. More generally let $G = \mathbb{Z}_n$ where $n = kl$ with $k, l > 1$. Then $H < G$ where
$$H = \{0, k, 2k, \dots, (l-1)k\}.$$
6. Let $G = \mathrm{GL}(n, \mathbb{R})$, and H be all the upper-triangular elements of G. Then $H < G$.
7. There are also many other interesting subgroups of $\mathrm{GL}(n, \mathbb{R})$, for example

(a) $\mathrm{SL}(n,\mathbb{R}) := \{A \in \mathrm{GL}(n,\mathbb{R}) \mid \det A = 1\}$.
(b) $\mathcal{O}(n,\mathbb{R}) := \{A \in \mathrm{GL}(n,\mathbb{R}) \mid A^T = A^{-1}\}$.
See [J, §5.2].

2.4.6. **Important notation.**

- When dealing with a general group G, as much as possible we will write gh for $g * h$.

We do this since it is tedious to keep on writing $*$. However, dropping the $*$ can be a little dangerous. For example, when the group is $\mathbb{Z}$ or $\mathbb{Z}_n$ (under addition), if we write ab for $a * b$, then

$$ab := a * b = a + b.$$

This would imply that we are writing ab to mean 'add a and b'. Since you are so used to writing ab to mean 'multiply a and b', this will cause confusion. Hence, when we are dealing with groups under addition (like $\mathbb{Z}$ or $\mathbb{Z}_n$), it is helpful to keep the $*$ notation in (see for example §2.5.3(3) and §3.2.3 later). Nevertheless, when discussing a *general* group G, we will drop the $*$ as much as possible.

2.5. Order of elements

2.5.1. *Definition.* (Order of a group) A *finite group* G is one with only a finite number of elements. The *order* of a finite group, written $|G|$, is the number of elements in G. (Note that if X is a set, we also often write $|X|$ to be the number of elements in X.)

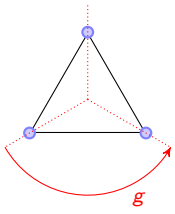
2.5.2. *Definition.* (Order of an element) [J, §6.3] Let G be a group and $g \in G$. Then the *order* $o(g)$ of g is the *least* natural number n such that

$$\underbrace{g * \ldots * g}_{n} = e.$$

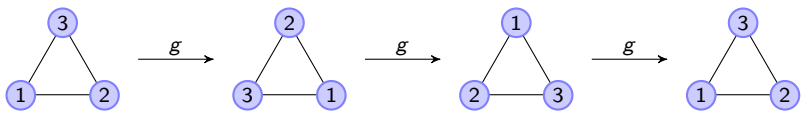
If no such n exists, we say that g has infinite order.

2.5.3. *Examples.*

1. From §1.3.2 $|D_n| = 2n$. From §1.4.1 $|S_n| = n!$
2. In D_3, if g is defined as before as



then



Thus $g^t \neq e$ for $1 < t < 3$ and $g^3 = e$, and so $o(g) = 3$.

3. Consider $1 \in \mathbb{Z}$. Then $1 * 1 = 1 + 1 = 2$, $1 * 1 * 1 = 3$,..., and so
$$\underbrace{1 * \ldots * 1}_{n} = n \neq 0 = e$$
for any $n > 0$. Hence $1 \in \mathbb{Z}$ has infinite order.
4. See Problems 2.13 – 2.18 for many examples of finite order.

2.5.4. *Theorem.* In a finite group, every element has finite order.

Proof. Let $g \in G$. Consider the infinite sequence $g, g^2, g^3, \ldots$. If G is finite, then there must be repetitions in this infinite sequence. Hence there exists $m, n \in \mathbb{N}$ with $m > n$ such that $g^m = g^n$. By cancelation (§2.1.3 part 1), $g^{m-n} = e$. This shows that $o(g) \leq m - n$, and so consequently $o(g)$ is finite. □

2.5.5. *Corollary.* Let g be an element of a finite group G. Then there exists $k \in \mathbb{N}$ such that $g^k = g^{-1}$.

Proof. By §2.5.4 there exists $t \in \mathbb{N}$ such that $g^t = e$. Applying g^{-1} to both sides gives $g^{t-1} = g^{-1}$. □

2.6. **Cyclic subgroups**

The easiest type of subgroup. See [J, §6].

2.6.1. *Definition.* If G is a group, $g \in G$ and $k \in \mathbb{Z}$, define
$$g^k := \begin{cases} \overbrace{g \ldots g}^{k} & \text{if } k > 0 \\ e & \text{if } k = 0 \\ \underbrace{g^{-1} \ldots g^{-1}}_{-k} & \text{if } k < 0 \end{cases}$$
and further define
$$\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}.$$
If G is finite, then $\langle g \rangle$ (being a subset of G) is finite, and we can think of $\langle g \rangle$ as
$$\langle g \rangle = \{e, g, \ldots, g^{o(g)-1}\}$$
by §2.5.4 and §2.5.5.

2.6.2. *Lemma.* If G is a group and $g \in G$, then $\langle g \rangle$ is a subgroup of G.

Proof. (sketch) Use the test for a subgroup §2.4.3. Make sure that you can do this, see also [J, §6.2]. In your proof, it is useful to note the fact that $g^a g^b = g^{a+b}$ for all $a, b \in \mathbb{Z}$. Although easy (it follows directly from the axioms of a group), the proof of this fact is tedious since it involves splitting into cases depending whether a (and b) are positive, negative or zero. □

2.6.3. *Definition.* A subgroup $H \leq G$ is *cyclic* if $H = \langle h \rangle$ for some $h \in H$. In this case, we say that H is the *cyclic subgroup generated by* h. If $G = \langle g \rangle$ for some $g \in G$, then we say that the group G is *cyclic*, and that g is a *generator*.

2.6.4. *Examples.*

1. $\mathbb{Z}_n$ (under addition) is cyclic, since $\langle 1\rangle = \mathbb{Z}_n$.
2. In $\mathbb{Z}_8$ the cyclic subgroup generated by 2 is $\langle 2\rangle = \{0, 2, 4, 6\}$. This is strictly contained in $\mathbb{Z}_8$.
3. In D_n, the subgroup H consisting of the identity and all the rotations, i.e.
$$H = \{e, g, g^2, \dots, g^{n-1}\}$$
is a cyclic subgroup since $H = \langle g\rangle$. Note also that $H = \langle g^{-1}\rangle$.

2.6.5. *Remarks.*

1. If $g \in G$, then by the line above §2.6.2, $o(g) = |\langle g\rangle|$, i.e. the order of an element equals the order of the subgroup that it generates.
2. If G is cyclic then necessarily G is abelian. See Problem 2.5. In particular, D_3 is not cyclic, since we calculated in §1.3.1 that $gh \neq hg$.
3. Let G be a finite group. Then
$$G \text{ is cyclic } \iff G \text{ contains an element of order } |G|.$$
Proof. ($\Leftarrow$) Suppose $g \in G$ has order $|G|$. Then $\langle g\rangle \leq G$ with $|\langle g\rangle| = |G|$ by 1. Hence $\langle g\rangle$ and G have the same number of elements, so $\langle g\rangle = G$.
($\Rightarrow$) Suppose $G = \langle g\rangle$ is cyclic, then counting the number of elements on both sides gives $|G| = |\langle g\rangle|$. By 1, this means that g has order $|G|$. □

This gives another proof that D_3 is not cyclic, since it has no element of order 6. The only possible orders are 1 (the identity), 3 (the two rotations) and 2 (the three reflections).

We next investigate how cyclic groups behave with respect to our previous constructions in §2.4 (subgroups) and §2.3 (product groups).

2.6.6. *Theorem.* Let G be a cyclic group and let H be a subgroup of G. Then H is cyclic.

Proof. If $H = \{e\}$ then trivially $H = \langle e\rangle$ and so H is cyclic. Hence we assume that $H \neq \{e\}$. In this case, H contains some non-identity element of G, i.e. $g^t \in H$ for some $t \neq 0$. Since H is closed under inverses, H also contains g^{-t}. Thus since either t or $-t$ is positive, H contains g^s for some $s > 0$. Now choose the *smallest* $s > 0$ such that $g^s \in H$ but $g^k \notin H$ for $1 \leq k \leq s-1$. We claim that $H = \langle g^s\rangle$.

First, since $g^s \in H$ and H is closed under inverses and products, the inequality $\langle g^s\rangle \subseteq H$ holds. For the reverse inequality, let $h \in H$ be arbitrary. Viewing h in G, $h = g^m$ for some $m \in \mathbb{Z}$. We will show (by contradiction) that m is a multiple of s, since then $h \in \langle g^s\rangle$, and so since h was arbitrary this shows $H \subseteq \langle g^s\rangle$, finishing the proof. If m is not a multiple of s, then we can write $m = qs + r$ for some $g \in \mathbb{Z}$ and some $0 < r < s$. Thus
$$g^m = g^{qs+r} = (g^s)^q g^r$$
and so
$$g^r = \underbrace{g^m}_{\in H}\underbrace{(g^s)^{-q}}_{\in H} \in H.$$

Since $0 < r < s$ and s was chosen *smallest* such that $g^s \in H$, this is a contradiction. □

Thus by above any subgroup of any cyclic group is also cyclic. However, products of cyclic groups are not so well behaved.

2.6.7. *Theorem.* Let $m, n \in \mathbb{N}$, let $G = \langle g \rangle$ be a cyclic group of order m and $H = \langle h \rangle$ be a cyclic group of order n. Then

$$G \times H \text{ is cyclic } \iff m \text{ and } n \text{ are coprime (i.e. } \gcd(m, n) = 1).$$

Proof. Recall that $G \times H$ has $|G||H| = mn$ elements.
($\Leftarrow$) Suppose m, n are relatively prime and let $x = (g, h)$. Then $x^k = (g^k, h^k)$, so

$$x^k = e_{G\times H} \iff (g^k, h^k) = (e_G, e_H) \iff g^k = e_G \text{ and } h^k = e_H.$$

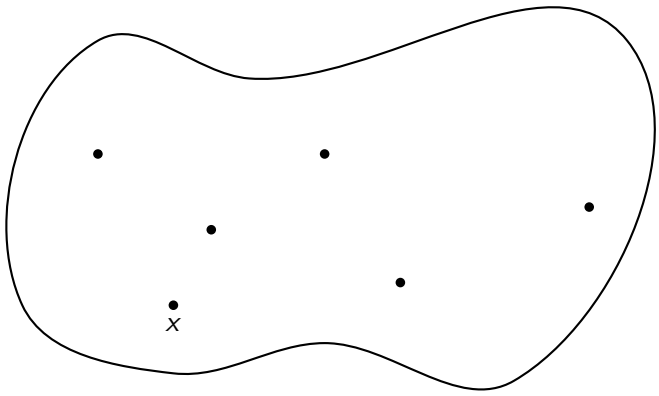
But the smallest such k (since $\gcd(m, n) = 1$) is mn. Hence x has order mn in the group $G \times H$ of mn elements. By §2.6.5(3), $G \times H$ is cyclic.
($\Rightarrow$) (by contrapositive) Conversely, suppose that $\gcd(m, n) = q > 1$. Then $k := \frac{mn}{q}$ is a multiple of both m and n. Thus if $(x, y) \in G \times H$, then $(x, y)^k = (x^k, y^k) = (e, e) = e_{G\times H}$. Hence $G \times H$ has no element of order mn, and so therefore again by §2.6.5(3) it cannot be cyclic. □

3. Lagrange's Theorem and Applications

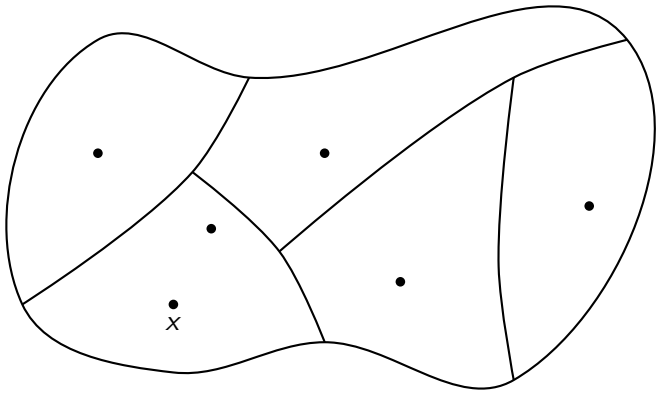
We now build up to Lagrange's Theorem, the first main theorem of this course.

3.1. **Recap on Equivalence relations**

Recall [L, §18] and [J, §8]. Intuitively, we often think of sets schematically as blobs



containing elements, drawn as dots. For various reasons, often we want to *partition* this set into smaller pieces, which we draw as



Whenever we need to partition a set into pieces in this way, the tool to use is an *equivalence relation*.

3.1.1. *Definition.* [L,§18] Let X be a set, and R a subset of $X \times X$ (thus R consists of some ordered pairs (s, t) with $s, t \in X$). If $(s, t) \in R$ we write $s \sim t$ and say "s is related to t". We call $\sim$ a *relation* on X.

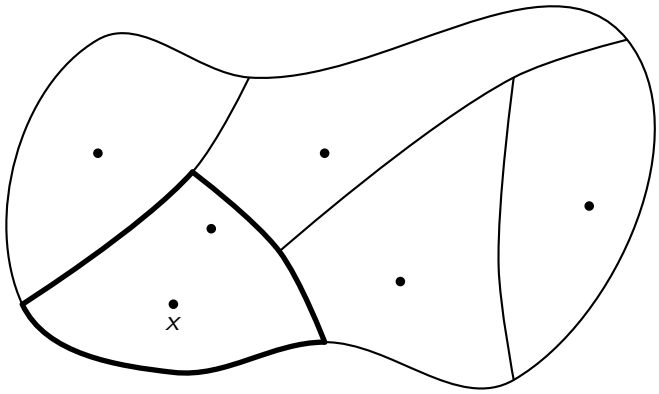
A relation $\sim$ is called an *equivalence relation* on X if

R. (Reflexive) $x \sim x$ for all $x \in X$

S. (Symmetric) $x \sim y$ implies that $y \sim x$ for all $x, y \in X$

T. (Transitive) $x \sim y$ and $y \sim z$ implies that $x \sim z$ for all $x, y, z \in X$.

The key point from Proofs and Problem Solving [L, 18.1] is that equivalence relations partition sets. If $\sim$ is an equivalence relation on a set X, then the set X is partitioned into pieces called the *equivalence classes*. In our previous picture



the bold highlighted piece is the equivalence class containing x, which *by definition* is just all elements that are related to x. It is denoted $\mathrm{cl}(x)$. In mathematical symbols, the bold highlighted piece is

$$\mathrm{cl}(x) := \{\textit{all elements that are related to } x\} = \{s \in X \mid x \sim s\}.$$

3.2. **Proof of Lagrange: cosets**

3.2.1. *Notation.* Let A, B be subsets of a group G and let $g \in G$. Then

$$AB := \{ab \mid a \in A, b \in B\}, \quad gA := \{ga \mid a \in A\},$$

and similarly for other obvious variants.

3.2.2. *Definition.* [J, §10.1] Let $H \leq G$ and let $g \in G$. Then a *left coset* of H in G is a subset of G of the form gH, for some $g \in G$.

3.2.3. *Example.* Consider $\mathbb{Z}_4$ under addition, and let $H = \{0, 2\}$. Recall $e = 0$. Now the cosets of H in G are

$$\begin{aligned}
eH = e * H &= \{e * h \mid h \in H\} = \{0 + h \mid h \in H\} = \{0, 2\}.\\
1H = 1 * H &= \{1 * h \mid h \in H\} = \{1 + h \mid h \in H\} = \{1, 3\}.\\
2H = 2 * H &= \{2 * h \mid h \in H\} = \{2 + h \mid h \in H\} = \{0, 2\}.\\
3H = 3 * H &= \{3 * h \mid h \in H\} = \{3 + h \mid h \in H\} = \{1, 3\}.
\end{aligned}$$

Hence there are two cosets, namely

$$0 * H = 2 * H = \{0, 2\} \quad \text{and} \quad 1 * H = 3 * H = \{1, 3\}.$$

The above shows that $g_1 H = g_2 H$ is possible, even when $g_1 \neq g_2$.

3.2.4. *Definition.* We denote G/H to be the set of left cosets of H in G.

As above in §3.2.3, usually the number of members of G/H (which we denote by $|G/H|$) is less than $|G|$. See §3.2.8 for the precise answer later.

3.2.5. *Lemma.* Suppose that $H \leq G$, then $|gH| = |H|$ for all $g \in G$.

Proof. There is an obvious map $H \to gH$ given by $h \mapsto gh$. It is clearly surjective, by definition of gH. It is injective by §2.1.3, since $gh_1 = gh_2$ implies that $h_1 = h_2$. □

3.2.6. *Theorem.* Let $H \leq G$.

1. For all $h \in H$, $hH = H$. In particular $eH = H$.
2. For $g_1, g_2 \in G$, the following are equivalent
   (a) $g_1H = g_2H$.
   (b) there exists $h \in H$ such that $g_2 = g_1h$.
   (c) $g_2 \in g_1H$.
3. For a fixed $g \in G$, the number of $g_1 \in G$ such that $gH = g_1H$ is equal to $|H|$.
4. For $g_1, g_2 \in G$, define $g_1 \sim g_2$ if and only if $g_1H = g_2H$. Then $\sim$ defines an equivalence relation on G.

Proof. 1. Since H is closed under multiplication, $hH \subseteq H$. For the reverse inclusion, suppose $t \in H$. Then $t = h(h^{-1}t)$ with $h^{-1}t \in H$. Hence $t \in hH$, and so $H \subseteq hH$.
2. (a) $\Rightarrow$ (c) Suppose that $g_1H = g_2H$, then $g_2 = g_2e \in g_2H = g_1H$.
(c) $\Rightarrow$ (b) This is true by definition of g_1H.
(b) $\Rightarrow$ (a) Suppose that there exists $h \in H$ such that $g_2 = g_1h$, then

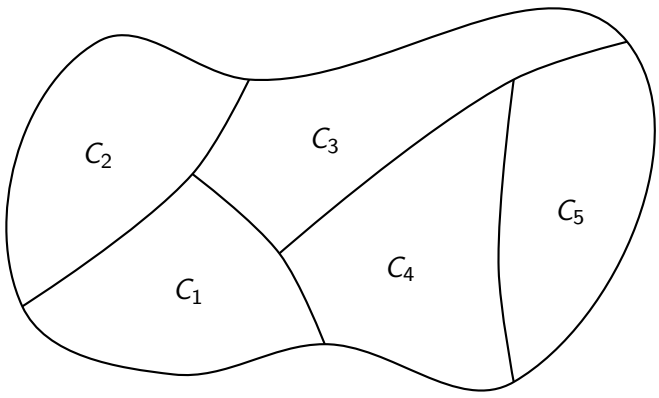
$$g_2H = (g_1h)H = g_1(hH) = g_1H$$

where the last equality is part 1.
3. By part 2, $gH = g_1H$ if and only if $g_1 \in gH$. Since $|gH| = |H|$ (by §3.2.5), there are precisely $|H|$ possibilities.
4. Is easy to verify using part 2. Make sure that you can do this. □

3.2.7. *Corollaries.* [J, §10] Suppose that G is a finite group.

1. **(Lagrange's theorem)** If $H \leq G$, then $|H|$ divides $|G|$.
2. Let $g \in G$. Then $o(g)$ divides $|G|$.
3. For all $g \in G$, we have that $g^{|G|} = e$.

Proof. 1. By §3.2.6 there is an equivalence relation $\sim$ defined on G. Thus G is partitioned into a (disjoint union) of the equivalence classes. Consequently we can count the elements of G by counting the elements in each piece of the partition, and



by doing this we obtain

$$|G| = \sum_{\text{equiv classes } C} |C| .$$

Now pick one of the C, then by definition of equivalence class $C = \mathrm{cl}(g)$ for some $g \in G$. By §3.2.6 part 3, the equivalence class containing g (i.e. C) has precisely $|H|$ members. Since C was arbitrary, every equivalence class has precisely $|H|$ members, and so

$$|G| = \underbrace{|H| + \ldots + |H|}_{\text{number of equiv classes}} = (\text{number of equiv classes}) \times |H| . \tag{1}$$

Hence $|H|$ divides $|G|$.

2. Just note that $\langle g \rangle$ is a subgroup of size $o(g)$, so apply part 1.

3. By part 2, say $|G| = k \times o(g)$. Then $g^{|G|} = (g^{o(g)})^k = e^k = e$. □

In the proof of Lagrange's Theorem, equation (1) shows that the number of equivalence classes is $\frac{|G|}{|H|}$. This then implies:

3.2.8. *Corollary.* $|G/H| = \frac{|G|}{|H|}$.

Proof. $|G/H|$ is equal to the number of *distinct* left cosets of H in G. But by definition of $\sim$, a conjugacy class consists of all those g which give the same left coset. Thus the number of equivalence classes is equal to the number of distinct left cosets, so using the proof of Lagrange we see that

$$|G| = (\text{number of equiv classes}) \times |H| = (\text{number of distinct left cosets}) \times |H| .$$

This shows that the number of distinct left cosets ($= |G/H|$) is equal to $\frac{|G|}{|H|}$. □

3.2.9. *Definition.* The *index* of $H \leq G$ is defined to be the number of *distinct* left cosets of H in G, which by above is $|G/H| = \frac{|G|}{|H|}$.

3.2.10. *Definition.* The *right cosets* of H in G are subsets of the form Hg.

3.2.11. *Properties.*

1. The properties of right cosets are entirely analogous to those of left cosets. We could alternatively prove Lagrange's Theorem by using right cosets.
2. If we prove everything above using right cosets, §3.2.8 would show that the number of distinct right cosets is equal to $\frac{|G|}{|H|}$. Hence the number of distinct right cosets is the same as the number of distinct left cosets, even although the right cosets might not be the same as the left cosets (see for example Problem 3.1).

3.3. **First applications of Lagrange**

3.3.1. *Theorem.* Suppose that G is a group with $|G| = p$, where p is prime. Then G is a cyclic group.

Proof. Choose $g \in G$ with $g \neq e$. Then $H := \langle g \rangle$ is a subgroup of G with at least two elements (e and g). But $|H|$ must divide $|G| = p$. Hence $|H| = p$ and so $H = G$. □

3.3.2. *Corollary.* Suppose that G is a group with $|G| < 6$. Then G is abelian.

Proof. If $|G| = 1$ then G is abelian (there is nothing to prove). If $|G| = 2$, 3 or 5 then G is cyclic (by 3.3.1) and hence abelian (by Problem 2.5). The only other case is $|G| = 4$. In this case, if G has an element of order four then it is cyclic, and hence abelian (by Problem 2.5). Therefore we can assume that G has no element of order four. Only the identity has order one, so by Lagrange (3.2.7 part 2) every non–identity element must have order two. Hence $g^2 = e$ for all $g \in G$, and so G is abelian (by Problem 2.8). □

We already know that the dihedral group D_3 has six elements (since $|D_n| = 2n$ by §1.3.2), and further D_3 is non-abelian (by 2.2.3 part 4). This tells you two things:

1. By the corollary, D_3 is the *smallest* example of a non-abelian group.
2. The corollary is 'best possible' in that the bound $|G| < 6$ cannot be improved.

The following two results are applications of Lagrange's Theorem to number theory.

3.3.3. *Theorem.* (Fermat's Little Theorem) If p is a prime and $a \in \mathbb{Z}$, then

$$a^p \equiv a \bmod p.$$

Proof. If $a \equiv 0$, then the result is obviously true, since then $a^p \equiv 0 \equiv a$. Hence we can assume that $a \not\equiv 0$, and so view a as an element of the group $\mathbb{Z}_p^* = \{z \in \mathbb{Z}_p \mid z \neq 0\}$ (which is a group under multiplication, with identity 1, see §1.2.6(6)). This group has precisely $p-1$ elements, so by Lagrange's Theorem §3.2.7(3) we deduce that $g^{p-1} = 1$ for all $g \in \mathbb{Z}_p$. Since $a \in \mathbb{Z}$ with $a \not\equiv 0$, viewing $a \in \mathbb{Z}_p^*$ it follows that $a^{p-1} \equiv 1 \bmod p$. Multiplying both sides by a yields the result. □

3.3.4. *Theorem.* If p is a prime, then

1. In $\mathbb{Z}_p^*$ only 1 and $p-1$ are their own inverses.
2. (Wilson's Theorem) $(p-1)! \equiv -1 \bmod p$.

Proof. 1. Clearly $1.1 = 1$ and $(p-1).(p-1) = p^2 - 2p + 1 \equiv 1 \bmod p$, so 1 and $p-1$ are their own inverses. Now take $1 < a < p-1$, then $0 < a-1 < p-2$ and $2 < a+1 < p$, so neither $a-1$ or $a+1$ is a multiple of p. As p is prime, the product $(a-1)(a+1) = a^2 - 1$ cannot be a multiple of p. Thus $a^2 \not\equiv 1 \bmod p$, so a is not its own inverse.

2. We first list the numbers

$$1 \qquad 2 \qquad 3 \qquad \cdots \qquad p-1$$

Since inverses are unique, and only 1 and $p-1$ are their own inverses (by part 1), we can pair off the remaining elements into inverse pairs

$$1 \qquad 2 \qquad 3 \qquad \cdots \qquad p-1$$

Hence mod p we have

$$(p-1)! = 1 \times 2 \times 3 \times \cdots \times (p-1) \equiv 1 \times (p-1) \equiv -1.$$

$$\equiv 1 \quad \equiv 1$$

□

4. Going between Groups

In linear algebra we study linear maps between vector spaces. In group theory, we study *homomorphisms* between groups.

4.1. Homomorphisms and Isomorphisms

This section covers [J, §9.1, §9.2].

4.1.1. *Definition.* Let G, H be groups. A map $\phi : G \to H$ is called a *group homomorphism* if

$$\phi(xy) = \phi(x)\phi(y) \quad \text{for all } x, y \in G.$$

(Note that xy on the left is formed using the group operation in G, whilst the product $\phi(x)\phi(y)$ is formed using the group operation in H.)

4.1.2. *Definition.* A group homomorphism $\phi : G \to H$ that is also a bijection is called an *isomorphism* of groups. In this case we say that G and H are *isomorphic* and we write $G \cong H$. An isomorphism $G \to G$ is called an *automorphism* of G.

4.1.3. *Remark.* An isomorphism thus matches up the two groups and their group operations perfectly. In other words, if G and H are isomorphic groups then they are *algebraically indistinguishable*. In the world of group theory, isomorphism is the idea of equality; we view two isomorphic groups as 'the same'.

4.1.4. *Examples.*

1. Consider $\mathbb{R}$ under addition and $\mathbb{R}^*_+$ (the group of positive real numbers) under multiplication. The map $\exp\colon \mathbb{R} \to \mathbb{R}^*_+$ is a group homomorphism since $\exp(x+y) = \exp(x)\exp(y)$. It is bijective, hence is an isomorphism.
2. If $n \in \mathbb{N}$, then every cyclic group of order n is isomorphic. (Proof: suppose $G = \langle g \rangle$ and $H = \langle h \rangle$ both have order n. The map $G \to H$ sending $g^t \mapsto h^t$ is a group homomorphism which is clearly bijective.) This is why we often refer to *the* cyclic group of order n.
3. Let $S_2 = \{e, \sigma\}$ where σ is the non-trivial permutation. We have $\sigma^2 = e$ and so $S_2 = \{e, \sigma\}$ is cyclic of order 2. Since $\mathbb{Z}_2$ is also cyclic of order 2, by part 2 we have $S_2 \cong \mathbb{Z}_2$.
4. More generally, every group of order 2 is isomorphic to $\mathbb{Z}_2$, since by §3.3.1 G is necessarily cyclic.
5. The map $\phi : D_3 \to S_3$ that takes a symmetry of the triangle to the corresponding permutation of the vertices is bijective. It is also a homomorphism of groups (one way to see this is to use the Cayley table in Problem 1.3

and check where every product gets sent to), hence it is an isomorphism, so $D_3 \cong S_3$.

4.1.5. *Lemma.* Let $\phi\colon G \to H$ be a group homomorphism. Then

1. $\phi(e) = e$ and further $\phi(g^{-1}) = (\phi(g))^{-1}$ for all $g \in G$.
2. If ϕ is injective, the order of $g \in G$ equals the order of $\phi(g) \in H$.

Proof. 1. Note first that $\phi(e) = \phi(ee) = \phi(e)\phi(e)$, hence by cancellation $\phi(e) = e$. For the second, note that

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e) = e = \phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$

and so $\phi(g^{-1})$ is an inverse for $\phi(g)$. Since inverses are unique, $\phi(g)^{-1} = \phi(g^{-1})$. 2. Since ϕ is a group homomorphism, $\phi(g^2) = \phi(g)\phi(g) = \phi(g)^2$. By induction $\phi(g^n) = \phi(g)^n$. Thus

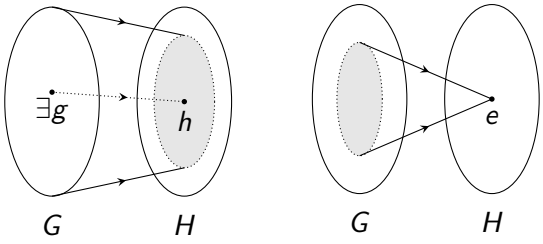
$$\phi(g)^n = e_H \overset{\text{part 1}}{\Leftrightarrow} \phi(g)^n = \phi(e_G) \Leftrightarrow \phi(g^n) = \phi(e_G) \overset{\phi \text{ inj}}{\Leftrightarrow} g^n = e_G$$

and so $\phi(g)$ and g have the same order. □

4.1.6. *Definition.* Let $\phi\colon G \to H$ be a group homomorphism.

1. The *image* of ϕ is defined to be
$$\operatorname{im}\phi := \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}$$
2. We define the *kernel* of ϕ to be
$$\operatorname{Ker}\phi := \{g \in G \mid \phi(g) = e_H\}.$$

In pictures, they are the shaded regions



$\operatorname{im}\phi$ $\operatorname{Ker}\phi$

Note that $\operatorname{im}\phi$ is a subgroup of H and that $\operatorname{Ker}\phi$ is a subgroup of G (use the test for a subgroup).

4.1.7. *Proposition.* Let $\phi\colon G \to H$ be a group homomorphism. Then

1. $\phi : G \to H$ is injective if and only if $\ker\phi = \{e_G\}$.
2. If $\phi : G \to H$ is injective, then ϕ gives an isomorphism $G \cong \operatorname{im}\phi$.

Proof. See Workshop 3. □

4.2. **Products and Isomorphisms**

We begin in §4.2.2 with an abstract isomorphism, then show in Examples §4.2.5 and §4.2.6 that this gives us very concrete examples of some isomorphic groups.

4.2.1. *Definition.* (reminder) If S and T are subsets of G, then we define

$$ST := \{st \,|\, s \in S,\ t \in T\}.$$

4.2.2. *Theorem.* [J, §14.3] Let $H, K \leq G$ be subgroups with $H \cap K = \{e\}$.

1. The map $\phi : H \times K \to HK$ given by $\phi : (h, k) \mapsto hk$ is bijective.
2. If further every element of H commutes with every element of K when multiplied in G (i.e. $hk = kh$ for all $h \in H, k \in K$), then HK is a subgroup of G, and furthermore it is isomorphic to $H \times K$, via ϕ.

4.2.3. *Remark.* The logic in the above is that H and K start life as given subgroups of G. However, we can simply regard them as groups in their own right and take their abstract product to form $H \times K$. Under the assumption that $H \cap K = \{e\}$, the conclusion of the first claim is that HK is a set which is bijective to $H \times K$. Under the further assumption that $hk = kh$ for all $h \in H, k \in K$, the second claim is that actually HK is a subgroup of G, and furthermore HK is the same as (=isomorphic to) $H \times K$ as groups, not just as sets.

Proof. 1. The map ϕ is surjective by definition. It is injective since if $hk = h'k'$ then $h'^{-1}h = k'k^{-1}$. But this element belongs to both H and K, hence it belongs to $H \cap K = \{e\}$. Thus $h'^{-1}h = k'k^{-1} = e$ and so $h = h'$ and $k = k'$.
2. Now assume that $hk = kh$ for all $h \in H, k \in K$. We check that HK is a subgroup of G. Clearly $e = ee \in HK$ and so $HK \neq \emptyset$. If $hk \in HK$ then $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK$. Finally if $hk, h'k' \in HK$ then so is $(hk)(h'k') = (hh')(kk')$. Now ϕ is a homomorphism of groups because

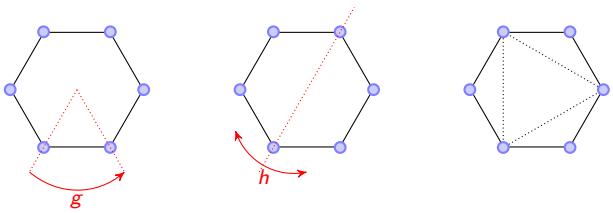
$$\phi((h, k) * (h', k')) = \phi(hh', kk') = hh'kk' = (hk)(h'k') = \phi(h, k)\phi(h', k')$$

(where we have written $*$ for the group operation in $H \times K$ and all other products are in G). Hence ϕ, being bijective by part 1, is a group isomorphism. □

4.2.4. *Corollary.* Let $H, K \leq G$ be finite subgroups of a group G with $H \cap K = \{e\}$. Then $|HK| = |H| \times |K|$.

Proof. Since HK is bijective to $H \times K$ by §4.2.2 (part 1), this is obvious (recall §2.3.3). □

4.2.5. *Example.* Consider D_6, the symmetries of a regular hexagon. Consider one of the equilateral triangles formed by the vertices of the hexagon.



Consider the set H consisting of those symmetries of the hexagon which are also symmetries of the triangle. Since H contains precisely the symmetries of the triangle, H is a subgroup of D_6 which is isomorphic to D_3. Explicitly,

$$H = \{e, g^2, g^4, h, g^2h, g^4h\} \cong D_3.$$

Now consider $K = \langle g^3 \rangle = \{e, g^3\}$, where $g^3 \in D_6$ is the half turn. This subgroup is isomorphic to $\mathbb{Z}_2$ (all groups of order two are) and further it intersects H trivially. The half turn commutes with all elements of H (since it commutes with g^2 and h) and so by §4.2.2 we deduce that $HK \cong H \times K \cong D_3 \times \mathbb{Z}_2$. Thus HK is a subgroup of D_6 with $6 \times 2 = 12$ elements, so since $|D_6| = 12$, necessarily $D_6 = HK$. Hence $D_6 \cong D_3 \times \mathbb{Z}_2$.

4.2.6. *More Examples.*

1. The group G of symmetries of the graph (e) in §1.1.2 has 4 elements. The reflection in the horizontal line generates a subgroup H with two elements which is thus isomorphic to $\mathbb{Z}_2$. Similarly for the reflection in the vertical line — it generates a subgroup K which is isomorphic to $\mathbb{Z}_2$. These two reflections commute, hence $HK \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Since $HK \subseteq G$ and both have four elements, $G = HK$ and so $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
2. Similarly, in the graph (b) in §1.1.2 there is a subgroup H isomorphic to S_3 from permuting the three danglers on the left, and a subgroup K isomorphic to $\mathbb{Z}_2$ from permuting the danglers on the right. Elements from these two subgroups commute, and so $HK \cong S_3 \times \mathbb{Z}_2$. Again by looking at the number of elements, $G = HK$ and so $G \cong S_3 \times \mathbb{Z}_2$.

5. Group Actions

One of the best way to study groups is to study how they act on other objects.

5.1. Definition of a group action

5.1.1. *Definition.* Let G be a group, and let X be a nonempty set. Then a (left) action of G on X is a map

$$G \times X \to X,$$

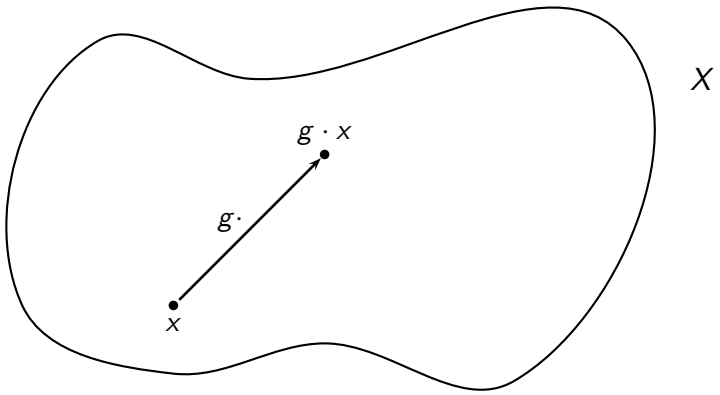
written $(g, x) \mapsto g \cdot x$, such that

$$g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \quad \text{and} \quad e \cdot x = x$$

for all $g_1, g_2 \in G$ and all $x \in X$.

The definition is dense, and a little hard to understand first time round. What it says is that if we take an element $g \in G$ and an element $x \in X$ (i.e. an element $(g, x) \in G \times X$), we can combine them to produce another element of X (the image of (g, x) under the map $G \times X \to X$), which we denote $g \cdot x$.

In our blob picture of the set X, if we pick $x \in X$, and $g \in G$, then these combine to produce some element $g \cdot x \in X$. We think of this as "g takes x to $g \cdot x$" and draw it



5.1.2. *Examples.*

1. Let G be the symmetry group of a graph, and let V be the set of vertices of the graph. We claim that G acts on V by $g \cdot x := g(x)$. The first axiom follows from properties of functions:

   $$g_1 \cdot (g_2 \cdot x) := g_1(g_2(x)) = (g_1 \circ g_2)(x) := (g_1 g_2) \cdot x$$

   for all $g_1, g_2 \in G$ and all $x \in X$. The second axiom follows since the identity e is the identity map, so it fixes every vertex.

Important special cases:

(a) The symmetric group S_n acts on the set $\{1, 2, \dots, n\}$.

(b) The group D_n acts on the set $\{1, 2, \dots, n\}$, where we think of the numbers as labelling the vertices of the n-gon.

2. Let G be the symmetry group of a graph, and let E be the set of edges of the graph. Then G acts on E, since if $e \in E$ connects vertices v_1 and v_2, define $g \cdot e :=$ the edge connecting $g(v_1)$ and $g(v_2)$. The two axioms follow in a similar way as above.
3. A group can act on many different sets. For example D_n acts on the set $\{1, 2, \dots, n\}$ as above. Alternatively, if we label the two faces of the n-gon T, B ("top" and "bottom"), then D_n also acts on the set $X := \{T, B\}$ where $g \in D_n$ acts by the identity if it leaves the n-gon the same way up (i.e. g is a rotation), and by swapping T, B if it turns it over (i.e. g is a reflection).
4. Let G be any group and X any (nonempty) set. Then $g \cdot x := x$ for all $g \in G$ and all $x \in X$ defines an action. We call this the *trivial action*. This action tells us no information, but it does always exist.
5. G acts on itself (i.e. take $X = G$), in many different ways. Three of these are

(a) 'Right action' defined $g \cdot h := hg^{-1}$ for all $g \in G$, $h \in X = G$. Thus the action is right multiplication by g^{-1}. Note carefully that the inverse g^{-1} appears. This ensures we get an action because

$$g_1 \cdot (g_2 \cdot h) = g_1 \cdot (hg_2^{-1}) = hg_2^{-1}g_1^{-1} = h(g_1g_2)^{-1} = (g_1g_2) \cdot h.$$

(b) 'Left action' defined $g \cdot h := gh$ for all $g \in G$, $h \in X = G$. Thus the action is left multiplication by g. Note that we do not require the inverse anymore, since

$$g_1 \cdot (g_2 \cdot h) = g_1 \cdot (g_2h) = g_1(g_2h) = (g_1g_2)h = (g_1g_2) \cdot h.$$

(c) 'Conjugate action' defined $g \cdot h := ghg^{-1}$ for all $g \in G$, $h \in X = G$.

5.2. **Faithful actions**

One of the nicest type of action. See [J,§15.2].

5.2.1. *Proposition.* Suppose G acts on X. Define

$$N := \{g \in G \mid g \cdot x = x \text{ for all } x \in X\}.$$

Then N is a subgroup of G.

Proof. We use the test for a subgroup. First, $e \in N$ since $e \cdot x = x$ for all $x \in X$, hence $N \neq \emptyset$. Further if $n_1, n_2 \in N$ then

$$(n_1n_2) \cdot x = n_1 \cdot (n_2 \cdot x) = n_1 \cdot x = x$$

for all $x \in X$ and so $n_1n_2 \in N$. Also, if $n \in N$ then

$$x = e \cdot x = (n^{-1}n) \cdot x = n^{-1} \cdot (n \cdot x) = n^{-1} \cdot x$$

for all $x \in X$ and so $n^{-1} \in N$. This show that N is a subgroup. □

5.2.2. *Definition.* Suppose that G acts on X, then the subgroup N defined above in §5.2.1 is called the *kernel* of the action. Note in [J] it is denoted $\operatorname{Ker}\cdot$, but this notation is quite hard to read. If $N = \{e\}$ then we say that the action is *faithful*.

Thus an action is faithful if $g \cdot x = x$ for all $x \in X$ implies that $g = e$. In words "the only member of G that fixes everything in X is the identity".

5.2.3. *Examples.*

1. Let G be the symmetry group of a graph acting on the set V of vertices. Only the identity fixes every vertex, so the action is faithful.
2. Let G be the rotational symmetry group of a Platonic solid acting on the set of faces. Again, only the identity fixes every face, so the action is faithful.
3. The action of D_n on the set $\{T, B\}$ in §5.1.2(3) is not faithful, since for example the rotation g fixes both T and B.

5.3. **Every group lives inside a symmetric group**

If X is a set, we denote

$$\operatorname{bij}(X) := \{\text{bijections } X \to X\}.$$

This is a group under composition of functions (just amend slightly the proof of §1.2.4). Note that if X is finite, then $\operatorname{bij}(X)$ is the symmetric group $S_{|X|}$, the symmetry group on $|X|$ letters.

5.3.1. *Lemma.* [J, 7.4] If G acts on a set X, then for all $g \in G$ the map

$$f_g \colon X \to X$$

defined $x \mapsto g \cdot x$ is a bijection.

Proof. Suppose that $f_g(x_1) = f_g(x_2)$, i.e. $g \cdot x_1 = g \cdot x_2$. Applying g^{-1} we have $g^{-1} \cdot (g \cdot x_1) = g^{-1} \cdot (g \cdot x_2)$. By the group action axioms, $(g^{-1}g) \cdot x_1 = (g^{-1}g) \cdot x_2$, so $e \cdot x_1 = e \cdot x_2$. Again by the group action axioms, $x_1 = x_2$. This shows injectivity.

Now let $x \in X$, and consider $y := g^{-1} \cdot x \in X$. Then

$$f_g(y) = g \cdot y = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e \cdot x = x,$$

which shows that f_g is surjective. Hence f_g is bijective. □

5.3.2. *Theorem.* [J, 7.4, 9.3] Let G be a group, and let X be a set. Then

1. An action of G on X is equivalent to a group homomorphism $\phi : G \to \operatorname{bij}(X)$.
2. The action is faithful if and only if ϕ is injective.
3. If the action is faithful, then ϕ gives an isomorphism of G with $\operatorname{im}\phi \leq \operatorname{bij}(X)$.

Proof. 1. Suppose that $\cdot$ defines an action, then define $\phi : G \to \operatorname{bij}(X)$ by $g \mapsto f_g$, where f_g is defined as in §5.3.1. We know that $f_g \in \operatorname{bij}(X)$ by 5.3.1, and further ϕ is a group homomorphism since

$$\phi(g_1g_2) = f_{g_1g_2} \text{ sends } x \mapsto (g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$$

whereas the composition of functions $\phi(g_1)\phi(g_2)$ sends $x \mapsto g_2 \cdot x \mapsto g_1 \cdot (g_2 \cdot x)$. Hence, as functions it follows that

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

Conversely, given a group homomorphism $\phi : G \to \mathrm{bij}(X)$, define $g \cdot x := \phi(g)(x)$. You can check that this gives a group action, and that these are inverse operations.
2. We have

$$\begin{aligned}
\phi \text{ is injective} &\overset{\S 4.1.7}{\iff} \ker \phi = \{e\} \\
&\iff \{g \in G \mid f_g = \mathrm{Id}\} = \{e\} \\
&\iff \{g \in G \mid f_g(x) = x \text{ for all } x \in X\} = \{e\} \\
&\iff \{g \in G \mid g \cdot x = x \text{ for all } x \in X\} = \{e\} \\
&\overset{\text{definition}}{\iff} \text{the action is faithful}
\end{aligned}$$

3. By part 2, there is an injective group homomorphism $\phi : G \to \mathrm{bij}(X)$, so the result follows from §4.1.7. □

5.3.3. *Corollary.* **(Cayley's Theorem)** Every finite group is isomorphic to a subgroup of a symmetric group.

Proof. The action of G on itself by left-multiplication ($g \cdot h = gh$) is faithful since if $g \neq e$ then $gh \neq h$. Thus by §5.3.2 part 3, G is isomorphic to a subgroup of $S_{|G|}$. □

5.3.4. *Examples.* Every finite group is isomorphic to a subgroup of a symmetric group, but not necessarily in a unique way.

1. By Cayley's Theorem, the group G of rotational symmetries of the dodecahedron (which turns out to have order 60, see Problem 5.12) is thus a subgroup of S_{60}. Thus we have embedded our group G into another group, of order 60!. Note that 60! is a *very* large number.

   But G also acts on the set X consisting of the 12 faces of the dodecahedron. This action is faithful, since every nontrivial symmetry clearly sends at least one face to a different one. Hence by §5.3.2 part 3, G is also a subgroup of $\mathrm{bij}(X) = S_{|X|} = S_{12}$.
2. Consider $C_3 = \{e, g, g^2\}$ acting on itself (as in Cayley's Theorem). Re-label $e \leftrightarrow 1$, $g \leftrightarrow 2$ and $g^2 \leftrightarrow 3$. Then the action of g on $X = G$ sends 1 to 2, 2 to 3, and 3 to 1, i.e. multiplication by g acts as the element

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

   on the set $G = X = \{1, 2, 3\}$. Thus in Cayley's Theorem, g gets sent to the element $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ of S_3. Hence

   $$C_3 = \langle g \rangle \cong \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rangle \leq S_3.$$

5.4. **Orbits and Stabilizers**

We build up to the next main theorem in the course, the orbit–stabilizer theorem (§5.4.12). This section covers [J, §7.2, §7.3].

5.4.1. *Definition.* Let G act on X, and let $x \in X$. The *stabilizer* of x is defined to be

$$\mathrm{Stab}_G(x) := \{g \in G \mid g \cdot x = x\}.$$

We will omit the G from the notation when it is clear what group we are considering.

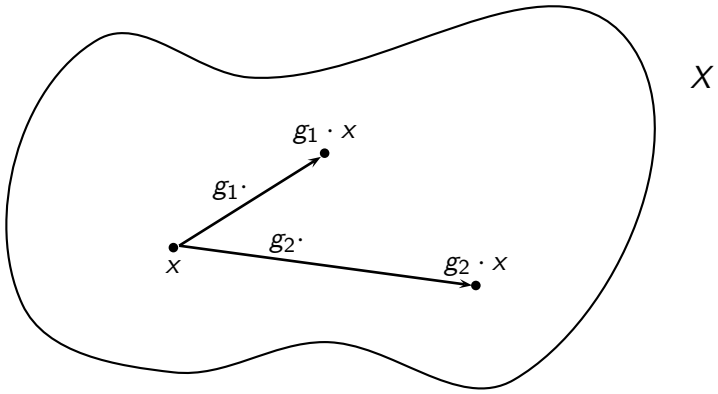
5.4.2. *Lemma.* For all $x \in X$, the stabilizer $\mathrm{Stab}_G(x)$ is a subgroup of G.

Proof. See Problem 5.5. □

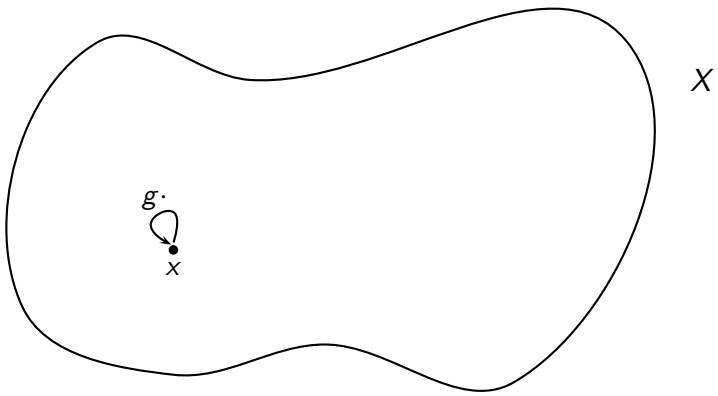
5.4.3. *Definition.* Let G act on X, and let $x \in X$. The *orbit* of x under G is

$$\mathrm{Orb}_G(x) = \{g \cdot x \mid g \in G\}.$$

In pictures:



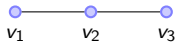
The orbit is all the elements of X that you can 'reach' from x by applying elements of G. In contrast, the stabilizer is all the elements of G that don't 'move' x, i.e. all those $g \in G$ for which



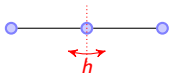
In particular, note that the orbit is a subset of X, and the stabilizer is a subset (in fact a subgroup) of G.

5.4.4. *Examples.*

1. Consider the symmetry group G of the graph



Then $G = \{e, h\}$ where



Thus

$$\begin{aligned} \mathrm{Orb}_G(v_1) &= \{g \cdot v_1 \mid g \in G\} = \{v_1, v_3\} \\ \mathrm{Orb}_G(v_2) &= \{g \cdot v_2 \mid g \in G\} = \{v_2\} \\ \mathrm{Orb}_G(v_3) &= \{g \cdot v_3 \mid g \in G\} = \{v_3, v_1\} \end{aligned}$$

and

$$\begin{aligned} \mathrm{Stab}_G(v_1) &= \{g \in G \mid g \cdot v_1 = v_1\} = \{e\} \\ \mathrm{Stab}_G(v_2) &= \{g \in G \mid g \cdot v_2 = v_2\} = \{e, h\} = G \\ \mathrm{Stab}_G(v_3) &= \{g \in G \mid g \cdot v_3 = v_3\} = \{e\}. \end{aligned}$$

2. Let $H \leq G$ and consider the 'right action' of H on $G = X$ defined by $h \cdot g := gh^{-1}$ (you need an inverse for the same reason as in §5.1.2(5)(a)). Then the orbit containing $g \in G$ is precisely

$$\mathrm{Orb}_H(g) = \{gh^{-1} \mid h \in H\} = \{gh \mid h \in H\} = gH.$$

Hence the orbits under this action are the left cosets of H in G. The stabilizer of $g \in G = X$ is

$$\mathrm{Stab}_H(g) = \{h \in H \mid gh^{-1} = g\} = \{e\}.$$

3. Let $H \leq G$ and consider the 'left action' of H on G defined by $h \cdot g := hg$. Then the orbit containing $g \in G$ is precisely

$$\{hg \mid h \in H\} = Hg.$$

Hence the orbits under this action are the right cosets of H in G.

4. See Problems 5.5 – 5.10 for more examples of orbits and stabilizers.

5.4.5. *Theorem.* [J, 8.4] Let G act on X. Then

$$x \sim y \iff y = g \cdot x \text{ for some } g \in G$$

defines an equivalence relation on X. The equivalence classes are the orbits of G. Thus when G acts on X, we obtain a partition of X into orbits.

Proof. Certainly $e \cdot x = x$ and so $x \sim x$. Next, suppose that $x \sim y$. Then there exists $g \in G$ such that $y = g \cdot x$, hence

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$

and so $y \sim x$. Finally, assume that $x \sim y$ and $y \sim z$. Then there exists $g, h \in G$ such that $y = g \cdot x$ and $z = h \cdot y$. Consequently

$$z = h \cdot y = h \cdot (g \cdot x) = (hg) \cdot x,$$

and so $x \sim z$. This shows that $\sim$ is an equivalence relation. The fact that the equivalence classes are the orbits follows straight from the definitions. □

5.4.6. *Example.* Continuing §5.4.4(1), G acts on the set of vertices $V = \{v_1, v_2, v_3\}$, and by our previous calculation, $\{v_1, v_3\} \cup \{v_2\}$ is the partition of V into orbits.

5.4.7. *Definition.* An action of G on X is *transitive* if for all $x, y \in X$ there exists $g \in G$ such that $y = g \cdot x$. Equivalently, X is a single orbit under G.

5.4.8. *Examples.*

1. For any given graph, as in §5.1.2 part 1 the group of symmetries acts on the set of vertices. This action may or may not be transitive (see Problem 5.3).
2. The dihedral group acts transitively on the set of vertices V of the n-gon. Let v_1, v_2 be vertices, then certainly there exists some rotation g^t for which $v_1 = g^t \cdot v_2$.

5.4.9. *Notation.* [J, top p87] Suppose G acts on X and $x, y \in X$. If y and x are in the same orbit,

$$\mathrm{send}_x(y) := \{g \in G \mid g \cdot x = y\}$$

is a non-empty subset of G.

5.4.10. *Proposition.* [J, p107] Let G act on X, let $x \in X$ and set $H := \mathrm{Stab}_G(x)$. If $y = g \cdot x$ for some $g \in G$ (i.e. y and x are in the same orbit), then

$$\mathrm{send}_x(y) = gH.$$

Proof. We show that $\mathrm{send}_x(y) \subseteq gH$, then $\mathrm{send}_x(y) \supseteq gH$.
($\subseteq$) Let $k \in \mathrm{send}_x(y)$, then by definition $k \cdot x = y$. Thus

$$(g^{-1}k) \cdot x = g^{-1} \cdot (k \cdot x) = g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$

so $g^{-1}k \in \mathrm{Stab}_G(x) := H$. By rules for cosets (§3.2.6) $k \in gH$.
($\supseteq$) Let $k \in gH$, so $k = gh$ for some $h \in H = \mathrm{Stab}_G(x)$. Then

$$k \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = y$$

so $k \in \mathrm{send}_x(y)$. □

Recall from §3.2.4 that if $H \leq G$ then we write G/H for the *set* (which might not be a group!) of left cosets of H in G.

5.4.11. *Theorem.* [J, p117] Let G act on X, let $x \in X$, and set $H := \mathrm{Stab}_G(x)$ Then the map

$$\mathrm{send}_x \colon \mathrm{Orb}_G(x) \to G/H \quad \text{which sends} \quad y \mapsto \mathrm{send}_x(y)$$

is a bijective map of *sets*.

Proof. Surjectivity: consider an arbitrary element $gH \in G/H$. Set $y := g \cdot x$, then certainly $y \in \mathrm{Orb}_G(x)$. By §5.4.10 $\mathrm{send}_x(y) = gH$, hence send_x is surjective.
Injectivity: suppose $y, z \in \mathrm{Orb}_G(x)$ such that $\mathrm{send}_x(y) = \mathrm{send}_x(z)$. Pick an element

$g \in \mathrm{send}_x(y) = \mathrm{send}_x(z)$. Then since $g \in \mathrm{send}_x(y)$, $y = g{\cdot}x$, and since $g \in \mathrm{send}_x(z)$, $z = g \cdot x$. Thus $y = g \cdot x = z$, hence $y = z$ and so send_x is injective. □

We arrive at one of the main results in this course.

5.4.12. *Corollary.* **(The orbit-stabilizer theorem)** Suppose G is a finite group acting on a set X, and let $x \in X$. Then $|\mathrm{Orb}_G(x)| \times |\mathrm{Stab}_G(x)| = |G|$, or in words

$$\text{size of orbit} \times \text{size of stabilizer} = \text{order of group}.$$

In particular, *the size of an orbit divides the order of the group.*

Proof. By §5.4.11 $|\mathrm{Orb}_G(x)| = |G/\mathrm{Stab}_G(x)|$. By §3.2.8 this is equal to $\frac{|G|}{|\mathrm{Stab}_G(x)|}$. □

The orbit–stabilizer theorem is useful both theoretically and computationally (see below, and the problem sheets, for both theory and nice applications), so it is very important.

5.4.13. *Some Practical Applications.*

1. (Order of the groups of rotational symmetries of Platonic solids) Let G be the rotational symmetry group of the tetrahedron. Consider G acting on the set F of four faces, and pick a face $f \in F$. Since the action is transitive (you can take any face to any other face just by rotating), $\mathrm{Orb}_G(f) = F$, so in particular $|\mathrm{Orb}_G(f)| = 4$. Also, the stabilizer $\mathrm{Stab}_G(f)$ consists of just the identity together with the rotations about the centre of that face. Thus

$$|G| = |\mathrm{Stab}_G(f)| \times |\mathrm{Orb}_G(f)| = 3 \times 4 = 12.$$

   A similar argument applies to all Platonic solids — see Problem 5.12.
2. See Workshop 4 for more practical applications.

On the other hand, as a theoretical application of the orbit–stabilizer theorem, we have the following.

5.4.14. *Theorem.* **(Cauchy's Theorem)** Let G be a group, p be a prime. If p divides $|G|$, then G contains an element of order p.

Proof. Set $G = \mathbb{Z}_p$. We divide the proof into steps

1. Consider the set

$$X := \{(g_0, g_1, \dots, g_{p-1}) \in \underbrace{G \times \dots \times G}_{p} \mid g_0 g_1 \dots g_{p-1} = e\}.$$

   Then $|X| = (|G|)^{p-1}$ since the first $p-1$ elements $g_0, \dots, g_{p-2}$ can be arbitrary and then there is one and only one g_{p-1} such that $(g_0 \dots g_{p-2})g_{p-1} = e$ (by §2.1.1).
2. We next claim that

$$k \cdot (g_0, g_1, \dots, g_{p-1}) := (g_k, g_{k+1}, \dots, g_{p-1}, g_0, \dots, g_{k-1})$$

defines an action of the group $G = \mathbb{Z}_p$ on X. The key is to show that $k \cdot (g_0, g_1, \dots, g_{p-1}) \in X$, as the remaining axioms are easy. This is just because

$$(g_0 \cdots g_{k-1})(g_k \cdots g_{p-1}) = e \iff (g_k \cdots g_{p-1})(g_0 \cdots g_{k-1}) = e,$$

since an element always commutes with its own inverse.

3. Note that the orbits of size one are those of the form $\{(g, g, \dots, g)\}$ where $g^p = e$.
4. Since $|Z_p| = p$, by orbit-stabilizer (applied to the action of $\mathbb{Z}_p$ on the set X) every orbit has size 1 or size p, since its size must divide $|\mathbb{Z}_p| = p$. Since orbits partition X,

$$|X| = \sum_{\text{orbits } O_i} |O_i|$$

Certainly there is at least one orbit of size one (namely $(e, e, \dots, e)$), so

$$|X| = 1 + \sum_{\text{all other orbits}} |O_i| \tag{2}$$

Now by step 1, $|X|$ is a multiple of p, so if all of the remaining orbits have size p, the equation (2) gives a contradiction. Hence at least one other orbit must have size one, so by step 3 there exists at least one $g \neq e$ with $g^p = e$.

This shows that $o(g) \leq p$, in fact it shows that p must be a multiple of $o(g)$ by [J, Thm 3(iii), p60]. Since p is prime and $o(g) \neq 1$, it follows that $o(g) = p$. □

See Problem 5.16 for another theoretical application of the orbit–stabilizer theorem.

5.5. **Pólya counting**

A beautiful application of group theory.

5.5.1. *Theorem.* [J, 11.3] Let G be a finite group acting on a finite set X. For $g \in G$ define

$$\mathrm{Fix}(g) := \{x \in X \mid g \cdot x = x\}$$

(so that $|\mathrm{Fix}(g)|$ is the number of elements of X that g fixes). Then

$$\text{the number of orbits in } X = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|\,.$$

Proof. Consider the set

$$Z := \{(g, x) \mid g \cdot x = x\}.$$

We compute $|Z|$ in two different ways. Firstly, for each $g \in G$ there are $|\mathrm{Fix}(g)|$ possible x's and so $|Z| = \sum_{g \in G} |\mathrm{Fix}(g)|$. On the other hand, for each $x \in X$ there are $|\mathrm{Stab}(x)|$ possible g's, so $|Z| = \sum_{x \in X} |\mathrm{Stab}\,(x)|$. But by orbit–stabilizer $|\mathrm{Stab}(x)| = \frac{|G|}{|\mathrm{Orb}(x)|}$, and so on comparing expressions for $|Z|$ we see that

$$\sum_{g \in G} |\mathrm{Fix}(g)| = \sum_{x \in X} \frac{|G|}{|\mathrm{Orb}(x)|}.$$

and so

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| = \sum_{x\in X}\frac{1}{|\mathrm{Orb}(x)|}.$$

Finally, since orbits always partition X, this means we can split X into pieces $O_1, \ldots, O_n$. Thus we can write

$$\begin{aligned}
\sum_{x\in X}\frac{1}{|\mathrm{Orb}(x)|} &= \sum_{x\in O_1}\frac{1}{|\mathrm{Orb}(x)|} + \ldots + \sum_{x\in O_n}\frac{1}{|\mathrm{Orb}(x)|} \\
&= \left(\underbrace{\frac{1}{|O_1|} + \ldots + \frac{1}{|O_1|}}_{|O_1|}\right) + \ldots + \left(\underbrace{\frac{1}{|O_n|} + \ldots + \frac{1}{|O_n|}}_{|O_n|}\right) \\
&= 1 + \ldots + 1 \\
&= \text{the number of orbits in } X.
\end{aligned}$$

□

5.5.2. *Example.*

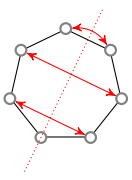
1. How many essentially different ways are there of colouring the vertices of a regular 7-gon with three colours? We will say that two colourings are the same if they can be made to coincide by an element of the dihedral group D_7. It is not required that every colouring uses all three colours.

   Examples include

   To solve this, we consider the action of D_7 on the set X of all $3^7 = 2187$ possible colourings. The problem just asks how many orbits there are, so by §5.5.1 we must analyse the fixed points.

   - The identity fixes every coloured 7-gon in X, so $|\mathrm{Fix}(e)| = 2187$.
   - Consider any non-trivial rotation (there are 6 of them). Clearly the only way a coloured 7-gon is fixed under the action of a rotation is if all the colours on all the vertices are the same. There are only 3 such diagrams.
   - Consider any reflection (there are 7 of them). Then for a coloured 7-gon to be fixed, the colour of the vertex through which the reflection line passes can be arbitrary, whereas the colours of the other vertices have to match up as in the following picture:

   Hence there are $3^4 = 81$ choices, and so 81 fixed points per reflection.

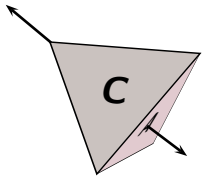
Hence by Pólya counting the number of orbits is equal to

$$\tfrac{1}{|G|}(2187 + \underbrace{3 + \ldots + 3}_{6} + \underbrace{81 + \ldots + 81}_{7}) = 198.$$

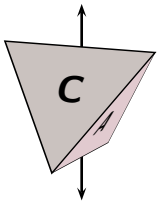
2. How many essentially different ways can a tetrahedron be coloured using n colours, each face being a single colour? (two colourings are regarded as the same if one can be obtained from the other by a rotational symmetry).

   By Workshop 2 we know that there are 12 rotational symmetries of the tetrahedron, and further we know their explicit form. The group of rotational symmetries G acts on the set X of all possible n^4 colourings. The question asks for the number of orbits, so by §5.5.1 we must analyse the fixed points.

   - The identity fixes everything, so $|\mathrm{Fix}(e)| = n^4$.
   - Consider a vertex–face rotation (of which there are eight).



     Then for a colouring to be fixed, the face through which the rotation takes place (A in the above picture) can have an arbitrary colour, whereas the remaining faces must all have the same colour. Thus the fixed set contains n^2 elements.
   - Consider an edge-edge rotation (of which there are three)



     For a colouring to be fixed, the face A in the picture must have the same colour as the back face that touches the bottom line. Similarly, the face C must have the same colour as the back face that touches the top line. Thus the fixed set contains n^2 elements.

   Hence by Pólya counting the number of orbits is equal to

$$\tfrac{1}{12}(n^4 + \underbrace{n^2 + \ldots + n^2}_{8} + \underbrace{n^2 + \ldots + n^2}_{3}) = \tfrac{1}{12}n^2(n^2 + 11).$$

5.5.3. *Remarks.*

1. See [J, §12], and also Workshop 5, for many other types of these problems.
2. Read [J, §12.1] for what 'essentially the same' should mean in this context.

6. Symmetric and Alternating Groups

The aim of this chapter is to describe the rotational symmetry groups of the Platonic solids. To do this will require some theory.

6.1. Symmetric and Alternating Groups

You are recommended to revise [J, §2] and [L, §20]. Recall

6.1.1. *Definition.* Let $n \in \mathbb{N}$, let $1 \leq r \leq n$ and let $\{a_1, a_2, \ldots, a_r\}$ be r distinct numbers between 1 and n. The *cycle* $(a_1\, a_2\, \ldots\, a_r)$ denotes the element of S_n that sends a_1 to a_2, a_2 to a_3, ..., a_{r-1} to a_r, a_r to a_1, and leaves the remaining $n - r$ numbers fixed. We say that the *length* of the cycle $(a_1\, a_2\, \ldots\, a_r)$ is r.

It is clear that our choice of starting point for the cycle is irrelevant, so e.g. $(a_1\, a_2\, \ldots\, a_r) = (a_2\, \ldots\, a_r\, a_1)$ etc.

6.1.2. *Definition.* Two cycles $(a_1\, a_2\, \ldots\, a_r)$ and $(b_1\, b_2\, \ldots\, b_s)$ are *disjoint* if

$$\{a_1, a_2, \ldots, a_r\} \cap \{b_1, b_2, \ldots, b_s\} = \emptyset.$$

6.1.3. *Note.* Composition of disjoint cycles is commutative (prove this — see Problem 6.1) and so e.g. $(1534)(27) = (27)(1534)$.

The following is [L, 20.3].

6.1.4. *Theorem.* Every permutation can be written as a product of disjoint cycles.

Proof. I will do this in one example, from which you will probably be able to write down the general proof yourself (if not, consult [L, §20]). Consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 4 & 1 & 3 & 6 & 2 & 9 & 8 \end{pmatrix}.$$

Start with the number 1. Tracing through, $1 \mapsto 5 \mapsto 3 \mapsto 4 \mapsto 1$ and we are back where we started. Next, choose the lowest number which does not appear in this cycle. Here, that is 2. Tracing through, $2 \mapsto 7 \mapsto 2$ and again we are back at where we started. Next, choose the lowest number which does not appear in the last two cycles — here that is 6. Tracing through, 6 gets sent to itself. Next, choose the smallest number that has not yet appeared. This is 8, and tracing through $8 \mapsto 9 \mapsto 8$. Thus

$$\sigma = (1534)(27)(6)(89).$$

□

6.1.5. *Note.* Since *disjoint* cycles commute, above we could equally write

$$\sigma = (1534)(27)(6)(89) = (6)(89)(27)(1534)$$

etc, in any order.

6.1.6. *Definition.* Given $\sigma \in S_n$, write σ as a product of disjoint cycles, as in §6.1.4. In this product, for each $t = 1, \dots, n$ let m_t denote the number of cycles of length t. Then we say that σ has *cycle type*

$$\underbrace{1, \dots, 1}_{m_1}, \underbrace{2, \dots, 2}_{m_2}, \dots, \underbrace{n, \dots, n}_{m_n},$$

As notation for cycle type, we usually abbreviate this to $1^{m_1}, 2^{m_2}, \dots, n^{m_n}$.

For an equivalent way of defining cycle type, see Problem 6.4.

6.1.7. *Examples.* In S_4, the element $(123)(4)$ has cycle type 1,3. The element (1234) has cycle type 4. The identity $e = (1)(2)(3)(4)$ has cycle type 1^4.

6.1.8. *Theorem.* The number of elements of S_n of cycle type $1^{m_1}, 2^{m_2}, \dots, n^{m_n}$ is

$$\frac{n!}{m_1! \dots m_n! 1^{m_1} 2^{m_2} \dots n^{m_n}}.$$

Proof. See Problem 6.2. □

6.1.9. *Examples.*

1. How many elements of type $1^2, 3, 4$ are there in S_9? Well, $m_1 = 2, m_3 = 1, m_4 = 1$ and all other m's are equal to zero. By the formula, there are $\frac{9!}{2.1.1.1^2.3^1.4^1} = 15120$ such elements.
2. The three possible cycle types in S_3 are 1^3, and $1, 2$, and 3. By the formula, these contain one, three and two elements respectively.

If you now reread [L, §20], especially the definition of even permutations [L, p173], you might see that it can all be expressed in the language of group actions:

6.1.10. *Definition.* Let $n \in \mathbb{N}$ and set

$$P = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Let $X = \{P, -P\}$. Then S_n acts on X by

$$\sigma \cdot P = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)})$$

If $\sigma \in S_n$ has the property that $\sigma \cdot P = P$, we say that σ is *even*. If $\sigma \cdot P = -P$, we say that σ is *odd*.

6.1.11. *Theorem.* Let A_n denote the set of all even permutations in S_n. Then A_n is a subgroup of S_n, with $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$. We call A_n the *alternating group.*

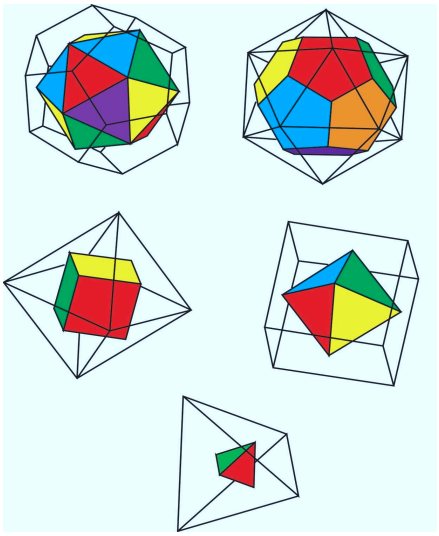
Proof. S_n acts on X, and $P \in X$. Then $A_n = \mathrm{Stab}_{S_n}(P)$ and so it is a subgroup of S_n (by §5.4.2). Since $\mathrm{Orb}(P) = \{P, -P\}$, $|\mathrm{Orb}(P)| = 2$. By the orbit-stabilizer theorem $|\mathrm{Orb}(P)| \times |\mathrm{Stab}(P)| = |S_n|$, thus $2 \times |A_n| = |S_n|$. □

6.1.12. *Example.* The group A_4 consists of the identity, eight 3-cycles and three elements of cycle type 2, 2. Explicitly, these are

$$e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23).$$

6.2. **Application to Platonic Solids**

On every Platonic solid, draw a dot at the centre of each face, and connect two dots if the faces meet at an edge. We call the resulting polytope the *dual*. Doing this[1], we obtain



So for example, the cube duals to the octahedron, which then duals back to the cube. Hence we can draw a cube inside an octahedron inside a cube. Because of this,

$$\text{symm of (outer) cube} \subseteq \text{symm of octahedron} \subseteq \text{symm of cube}$$

and thus we have equality throughout. This shows that the symmetries of the cube gives the same group as symmetries of the octahedron (its dual). In exactly the same way, the symmetries of the dodecahedron give the same group as the symmetries of the icosahedron.

Thus, to determine the rotational symmetry groups of all the Platonic solids, we need only determine

1. The rotational symmetry group of the tetrahedron.
2. The rotational symmetry group of the cube.
3. The rotational symmetry group of the dodecahedron.

We consider each in turn:

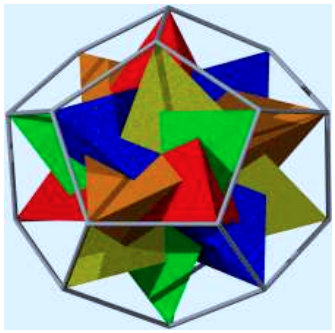
6.2.1. *The cube.* Consider the group G of rotational symmetries of the cube, acting on the set X of diagonals of the cube. Note that $|X| = 4$. This gives us a group homomorphism $\phi : G \to S_4 = S_{|X|}$, as in §5.3.2. Now no non-identity element of the cube fixes all the diagonals (we know all 24 rotational symmetries, so just check

[1] Image from http://xploreandxpress.blogspot.co.uk/2011/05/fun-with-mathematics-art-and-science-of.html

each), hence the action is faithful. Again, by §5.3.2 this shows that $G \cong \operatorname{Im}\phi \leq S_4$. Since we already know that $|G| = 24$, this means that $\operatorname{Im}\phi$ is a subset of S_4 with 24 elements. But $|S_4| = 4! = 24$, so $\operatorname{Im}\phi = S_4$. Hence $G \cong S_4$ (via ϕ).

6.2.2. *The tetrahedron.* Let G be the group of rotational symmetries of the tetrahedron. Then G acts on the set X of 4 vertices, thus as in §5.3.2 we have a group homomorphism $\phi : G \to S_4 = S_{|X|}$. The only symmetry which fixes all the vertices is the identity, hence ϕ is injective and so again $G \cong \operatorname{Im}\phi$. Now all members of G give an even permutations of the vertices (since rotations about a vertex give 3-cycles and rotations about midpoints of opposite edges have cycle-type 2,2), hence $G \cong \operatorname{Im}\phi \leq A_4$. Since $|\operatorname{Im}\phi| = |G| = 12 = |A_4|$, necessarily $\operatorname{Im}\phi = A_4$ and so $G \cong A_4$.

6.2.3. *The dodecahedron.* This is harder, but only because it is a little more difficult to visualize. Pack the dodecahedron with 5 tetrahedron[2], as in



Let G be the group of rotational symmetries of the dodecahedron, then G acts on the set X of 5 tetrahedron. Exactly as above we have a group homomorphism $\phi : G \to S_5 = S_{|X|}$, and the same strategy shows that $G \cong A_5$.

[2]Image from http://davidf.faricy.net/polyhedra/platonic_solids.html

7. Conjugacy and Normal Subgroups

In §7.1 we basically let G act on itself, then apply the results of the last sections. This then leads to normal subgroups [J, §13, §15].

7.1. Conjugate elements

7.1.1. *Definition/ Lemma.* Let $h \in G$ and $g \in G := X$. Then

$$h \cdot g := hgh^{-1}$$

defines an action of a group G on itself, called the *conjugation action*. The orbits are called the *conjugacy classes* of G. Under this action, the stabilizer of an element $g \in G$ is precisely

$$C(g) := \{h \in G \mid gh = hg\}.$$

which we define to be the *centralizer* of g in G.

Proof. To check this is a group action, note that $e \cdot g = ege^{-1} = g$ and also that

$$h \cdot (k \cdot g) = h \cdot (kgk^{-1}) = hkgk^{-1}h^{-1} = (hk)g(hk)^{-1} = (hk) \cdot g.$$

To see that the stabilizer of g is $C(g)$ we simply note that

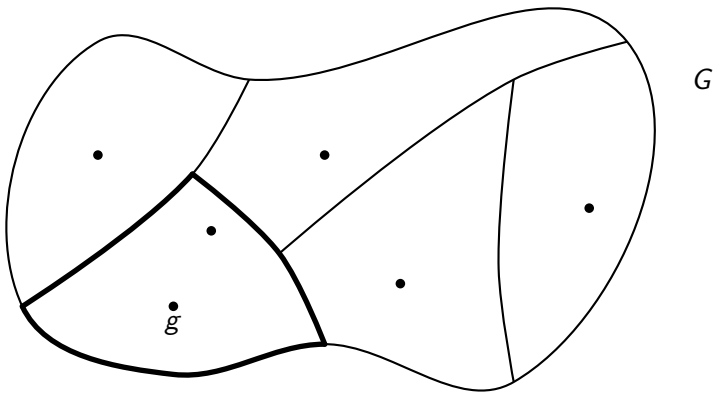
$$h \in \mathrm{Stab}_G(g) \iff h \cdot g = g \iff hgh^{-1} = g \iff hg = gh \iff h \in C(g).$$

□

7.1.2. *Examples of conjugacy classes.*

1. See Problem 6.14 for the conjugacy classes in D_4.
2. See §7.2 for conjugacy in the symmetric group S_n.

Orbits of a group action of G on X always partition the set X (§5.4.5). Since here $X = G$, the orbits of the conjugacy action (=the conjugacy classes) partition G, so we can draw:



where the bold highlighted piece is the conjugacy class containing g. By definition it contains all the elements that are in the same orbit as g, i.e. all the elements $h \cdot g$ as h runs through the elements of G. In mathematical symbols, the bold piece is thus

$$\{hgh^{-1} \mid h \in G\}.$$

7.1.3. *Definition.*

1. We say that g, g' are *conjugate* if there exists $h \in G$ such that $g' = hgh^{-1}$. That is, two elements are conjugate if they lie in the same conjugacy class.
2. [J, 13.5] We define the *centre* of a group G to be

$$C(G) := \{g \in G \,|\, gh = hg \text{ for all } h \in G\}.$$

   If $g \in C(G)$, we say that g is *central*.

It is easy to check that $C(G) = \bigcap_{g \in G} C(g)$, i.e. the centre of a group is the intersection of all the centralizers.

7.1.4. *Examples of centres of groups.*

1. G is abelian if and only if $C(G) = G$.
2. In $\mathrm{GL}(n, \mathbb{R})$ the centre is $\{\lambda \mathbb{I} \,|\, \lambda \in \mathbb{R}^*\}$. See Problem 6.12.

We obtain the following results entirely for free from the previous sections.

7.1.5. *Corollaries.*

1. For all $g \in G$, the centralizer $C(g)$ is a subgroup of G.
2. The centre $C(G)$ is a subgroup of G.
3. If G is finite and $g \in G$, then

$$(\text{the number of conjugates of } g \text{ in } G) \times |C(g)| = |G|\,.$$

4. $\{e\}$ is always a conjugacy class of G
5. $\{g\}$ is a conjugacy class if and only if $g \in C(G)$. Hence $C(G)$ is the union of all the one-element conjugacy classes.

Proof. 1. $C(g) = \mathrm{Stab}_G(g)$, and stabilizers are always subgroups (by §5.4.2).
2. Note $C(G) = \bigcap_{g \in G} C(g)$, and an intersection of subgroups is always a subgroup (Problem 2.4).
3. This is just the orbit-stabilizer theorem (§5.4.12).
4. If g is conjugate to e, then there exists $h \in G$ such that $g = heh^{-1}$, so $g = hh^{-1} = e$. Thus the only element conjugate to e is e itself.
5. $\{g\}$ is a conjugacy class $\iff$ the only element conjugate to g is g itself $\iff$ $g = hgh^{-1}$ for all $h \in G$ $\iff$ $gh = hg$ for all $h \in G$ $\iff$ $g \in C(G)$. □

The following is also just a special case of what we already know.

7.1.6. *Theorem.* Suppose that G is a finite group with conjugacy classes $C_1, \ldots, C_n$. We adopt the convention that $C_1 = \{e\}$. Let the conjugacy classes have sizes $c_1, \ldots, c_n$ (so that $c_1 = 1$).

1. If $g \in C_k$, then $c_k = \frac{|G|}{|C(g)|}$. In particular, c_k divides the order of the group.

2. We have
$$|G| = c_1 + c_2 + \ldots + c_n,$$
and further each of the c_j divides $|G|$. This is called the *class equation* of G.

Proof. Part 1 is just the orbit-stabilizer theorem (§5.4.12) applied to the conjugacy action. Part 2 is a trivial consequence of G being partitioned into conjugacy classes. Each c_j divides $|G|$ by part 1. □

7.1.7. *Examples.*

1. See Problems 6.15 – 6.16 for examples of the class equation.
2. See Problem 6.26 for the use of the class equation in a problem which doesn't seem to directly involve it.

The class equation has theoretical consequences. The proof of part one in the following should remind you of the argument in the proof of Cauchy's Theorem (§5.4.14).

7.1.8. *Theorem.*

1. If $|G| = p^k$ where p is prime and $k \in \mathbb{N}$, then $|C(G)| \geq p$.
2. Every group G of order p^2 (where p is prime) is abelian.

Proof. 1. Consider the class equation
$$|G| = c_1 + \ldots + c_n.$$
Every conjugacy class has size one or a positive power of p. Certainly $\{e\}$ is a conjugacy class of size one. Hence since p divides $|G|$, we must have at least $p-1$ more conjugacy classes of size one. The centre of G is the union of all the one-element conjugacy classes (by §7.1.5) and so the result follows.
2. By part 1 and Lagrange, $|C(G)|$ is either p or p^2. Suppose $|C(G)| = p$. Choose $g \notin C(G)$, then the centralizer $C(g)$ is strictly bigger than $C(G)$, since $g \in C(g)$. Hence $C(g) = G$, which in turn implies that $g \in C(G)$, a contradiction. Thus $|C(G)| \neq p$ and so $|C(G)| = p^2$. This implies that $C(G) = G$ and so the group is abelian. □

7.2. **Conjugacy in S_n is determined by cycle type**

7.2.1. *Lemma.* Let $\sigma \in S_n$, and write σ as a product of disjoint cycles, say $\sigma = (a_1 \ldots a_r)(b_1 \ldots b_s)\ldots$. Then for all $\tau \in S_n$,
$$\tau\sigma\tau^{-1} = (\tau(a_1)\ldots\tau(a_r))(\tau(b_1)\ldots\tau(b_s))\ldots$$
which is a product of disjoint cycles.

Proof. Since both sides are functions $\{1, \ldots, n\} \to \{1, \ldots, n\}$, we just have to check that the right hand side applied to every element in $\{1, \ldots, n\}$ gives the same answer as $\tau\sigma\tau^{-1}$ does. To see this, note for example that
$$\tau\sigma\tau^{-1}(\tau(a_1)) = \tau\sigma(a_1) = \tau(a_2)$$
and so $\tau\sigma\tau^{-1}$ sends $\tau(a_1)$ to $\tau(a_2)$. The other elements are checked similarly. □

7.2.2. *Theorem.* Two permutations in S_n are conjugate if and only if they have the same cycle type (up to ordering).

Proof. ($\Rightarrow$) is §7.2.1.
($\Leftarrow$) Let

$$\begin{aligned}\sigma &= (a_1 \dots a_r)(b_1 \dots b_s) \dots (f)(g)(h)\\ \gamma &= (\hat{a}_1 \dots \hat{a}_r)(\hat{b}_1 \dots \hat{b}_s) \dots (\hat{f})(\hat{g})(\hat{h})\end{aligned}$$

be elements of S_n with the same cycle type. Then

$$\{a_1, \dots, a_r, b_1, \dots, b_s, \dots, f, g, h\} = \{1, \dots, n\} = \{\hat{a}_1, \dots, \hat{a}_r, \hat{b}_1, \dots, \hat{b}_s, \dots, \hat{f}, \hat{g}, \hat{h}\}$$

in some order, with no repetitions. Define τ to be the element of S_n which sends $a_1 \mapsto \hat{a}_1, \dots, h \mapsto \hat{h}$. Now §7.2.1 shows that

$$\begin{aligned}\tau\sigma\tau^{-1} &= (\tau(a_1) \dots \tau(a_r))(\tau(b_1) \dots \tau(b_s)) \dots (\tau(f))(\tau(g))(\tau(h))\\ &= (\hat{a}_1 \dots \hat{a}_r)(\hat{b}_1 \dots \hat{b}_s) \dots (\hat{f})(\hat{g})(\hat{h})\\ &= \gamma\end{aligned}$$

thus $\tau\sigma\tau^{-1} = \gamma$ and so σ and γ are conjugate. □

7.2.3. *Examples.*

1. How many elements are conjugate to (123)(4567)(8)(9) in S_9? By §7.2.2, this is equal to the number of elements of cycle type $1^2, 3, 4$. By §6.1.9, this is equal to 15120.
2. By the above theorem and §6.1.9 part 2, we can work out all the conjugacy classes in S_3. Thus there are three conjugacy classes (since there are three cycle types), and so the conjugacy classes in S_3 are described by

cycle type	typical element	number of elements
1^3	e	1
$1, 2$	(1)(23)	3
3	(123)	2

You should perform a similar calculation for S_4, by doing Problem 6.19.

7.3. **Normal subgroups**

It turns out that analysing normal subgroups leads to the proof that a general quintic equation cannot be solved using a simple formula. For this reason, and many others, normal subgroups are important.

7.3.1. *Definition.* A subgroup N of G is *normal* if

$$gng^{-1} \in N \quad \text{for all } g \in G \text{ and all } n \in N.$$

We write $N \trianglelefteq G$ if N is a normal subgroup of G.

7.3.2. *Remark.*

1. If G is abelian, then every subgroup of G is normal.
2. $G \trianglelefteq G$ and $\{e\} \trianglelefteq G$.

7.3.3. *Theorem.* Let N be a subgroup in G, then N is a normal subgroup if and only if N is a union of conjugacy classes.

Proof. ($\Leftarrow$) Suppose that N is the union of conjugacy classes. Let $n \in N$ and $g \in G$, then certainly $gng^{-1} \in \{\text{conj class containing } n\} \subseteq N$ and so N is normal.
($\Rightarrow$) Suppose that N is normal. Then if $n \in N$, $gng^{-1} \in N$ for all $g \in G$, and so N contains the conjugacy class containing n. Therefore N contains the conjugacy classes of all its elements, so in particular N is a union of conjugacy classes. □

7.3.4. *Corollary.* If G is a group, then $C(G) \trianglelefteq G$.

Proof. We already know that $C(G)$ is a subgroup. Further $C(G)$ is the union of all one-element conjugacy classes by §7.1.5, so the result follows from §7.3.3. □

Other examples of normal subgroups:

7.3.5. *Lemma.*

1. Let $\phi : G \to H$ be a group homomorphism. Then $\ker \phi \trianglelefteq G$.
2. (Recall §5.2.1) Suppose that G acts on X, then the kernel of the action
$$N := \{g \in G \mid g \cdot x = x \text{ for all } x \in X\}$$
is a normal subgroup of G.

Proof. 1. This is an important exercise, see Problem 6.22.
2. In the proof of §5.3.2(2), we described N as the kernel of some group homomorphism. Hence 2 follows from 1. □

7.3.6. *Lemma.* Let $N \leq G$. Then the following are equivalent:

1. N is normal in G.
2. $gNg^{-1} = N$ for all $g \in G$.
3. $gN = Ng$ for all $g \in G$.

Proof. 1⇒3. Suppose that N is normal. Let $g \in G$, then for all $n \in N$, $gng^{-1} \in N$ so multiplying on the right by g shows that $gn \in Ng$. This shows that $gN \subseteq Ng$. On the other hand $g^{-1} \in G$ so $g^{-1}n(g^{-1})^{-1} \in N$, i.e. $g^{-1}ng \in N$. Multiplying on the left by g shows that $ng \in gN$. This holds for all $n \in N$, so $Ng \subseteq gN$. Combining gives $gN = Ng$.
3⇒2 and 2⇒1 are similar, see Problem 6.21. □

Sometimes, normal subgroups appear by luck!

7.3.7. *Theorem.* Let $H \leq G$ with $\frac{|G|}{|H|} = 2$. Then H is normal in G.

Proof. We know that there are precisely $\frac{|G|}{|H|} = 2$ distinct left cosets of H (by §3.2.8) so one must be H, the other $G\backslash H = \{g \in G \mid g \notin H\}$. Similarly, by the right coset version of §3.2.8, there are precisely $\frac{|G|}{|H|} = 2$ distinct right cosets of H, so one must be H, the other $G\backslash H = \{g \in G \mid g \notin H\}$. Hence for all $g \in G$,
$$gH = \begin{cases} H & \text{if } g \in H \\ G\backslash H & \text{if } g \notin H \end{cases} \qquad Hg = \begin{cases} H & \text{if } g \in H \\ G\backslash H & \text{if } g \notin H \end{cases}$$

and so $gH = Hg$ for all $g \in G$. By §7.3.6, H is normal in G. □

7.3.8. *Examples.*

1. $A_n \trianglelefteq S_n$ since $\frac{|S_n|}{|A_n|} = 2$ by §6.1.11.
2. The rotations $H := \{e, g, \dots, g^{n-1}\}$ form a cyclic subgroup of D_n. Since $\frac{|D_n|}{|H|} = 2$, necessarily $H \trianglelefteq D_n$.

7.3.9. *Definition.* We say that a group G is *simple* if the only normal subgroups of G are $\{e\}$ and G.

7.3.10. *Remark.* The group A_5 is a simple group by Problem 6.27 (or [J, 15.6]). It turns out that this is the reason why there is no formula giving the roots of a quintic equation $x^5 + ax^4 + \dots + e = 0$ (see the Jewels of Algebra course).

7.4. **Factor groups**

These are also known as quotient groups. This section is not examinable, but gives a bit of perspective.

Given a subgroup $H \leq G$, recall G/H denotes the set of left cosets of H in G, i.e. G/H is the set of all subsets of G of the form gH.

7.4.1. *Examples.*

1. $G = \mathbb{Z}_4$ and $H = \{0, 2\}$. Then by §3.2.3
$$G/H = \{\{0, 2\}, \{1, 3\}\}.$$
2. $G = \mathbb{R}^3$, and $H = x$-y plane. Then
$$G/H = \{\text{all planes parallel to } H\}.$$

Factor groups ask the question: is the set G/H a group?

7.4.2. *Theorem.* G/H is a group under $g_1H * g_2H := g_1g_2H \iff H$ is a normal subgroup of G.

Proof. ($\Rightarrow$) Suppose that $g_1N * g_2N := g_1g_2N$ defines an operation. Let $g \in G$ and $n \in N$. Then $gnN * g^{-1}N := gng^{-1}N$. But on the other hand $gnN = gN$ by rules for cosets, so $gnN * g^{-1}N = gN * g^{-1}N := gg^{-1}N = N$. This shows that $gng^{-1}N = N$, so by rules for cosets $gng^{-1} \in N$.
($\Leftarrow$) Suppose that N is normal. What is the problem?

Recall from Problem 1.1 that

$$f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \quad \text{sending} \quad (\tfrac{a}{b}, \tfrac{c}{d}) \mapsto \tfrac{a+c}{b+d}$$

is *not* a function. Since an operation on $\mathbb{Q}$ is the same thing as a function $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, it follows that $\frac{a}{b} * \frac{c}{d} := \frac{a+c}{b+d}$ is not an operation (see Problem 1.8).

Thus innocent–looking things need not be operations! Now we claim that $g_1N * g_2N := g_1g_2N$ is an operation, i.e. we claim that

$$f : G/H \times G/H \to G/H \quad \text{sending} \quad (g_1N, g_2N) \mapsto g_1g_2N$$

is a function. Exactly as in Problem 1.1 we need to check that

$$g_1N = g_2N \text{ and } h_1N = h_2N \quad \Rightarrow \quad g_1N * h_1N = g_2N * h_2N.$$

Now $g_1 = g_2n$ for some $n \in N$ and $h_1 = h_2m$ for some $m \in N$. Further $h_2^{-1}nh_2 \in N$ (since N is normal), so there exists $n' \in N$ such that $h_2^{-1}nh_2 = n'$, so $nh_2 = h_2n'$. Putting this together, we see that

$$g_1N * h_1N = g_1h_1N = g_2nh_2mN = g_2h_2n'mN = g_2h_2N = g_2N * h_2N,$$

as required. The group axioms are easy to check: the identity is $eN = N$ and the inverse of gN is $g^{-1}N$. □

The upshot is that when $N \trianglelefteq G$ we can form the *group* G/N, which is called the factor (or quotient) group. Being able to do this is one of the reasons why normal subgroups are so important—for example by passing to the group G/N (which is smaller) we are often able to use induction arguments. There are many other reasons why factor groups are great too, and I will discuss some in the lecture.

7.4.3. *Examples.*

1. $A_n \trianglelefteq S_n$ by §7.3.8, so we can form the group S_n/A_n. Since $|S_n/A_n| = \frac{|S_n|}{|A_n|} = 2$, and all groups of order two are isomorphic to $\mathbb{Z}_2$, necessarily $S_n/A_n \cong \mathbb{Z}_2$.
2. Consider $G = \mathbb{Z}$ with subgroup $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$. Since G is abelian, necessarily $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, so we can form the group $\mathbb{Z}/n\mathbb{Z}$. It turns out that this group is isomorphic to $\mathbb{Z}_n$, the integers mod n.

Now if $\phi\colon G \to H$ is a group homomorphism, then by §7.3.5 $\ker\phi \trianglelefteq G$ and so we can form the group $G/\ker\phi$. The first isomorphism theorem [J, 16.4] states that

$$G/\ker\phi \cong \operatorname{im}\phi.$$

Recall from linear algebra that if $f\colon V \to W$ is a linear map between vector spaces, then [P, p211] the rank–nullity theorem states that

$$\dim(\operatorname{im} f) = \dim V - \dim(\ker f).$$

This is really just a special case of the first isomorphism theorem.

Exercises

Section 1

Suitable Questions from Jordan and Jordan.

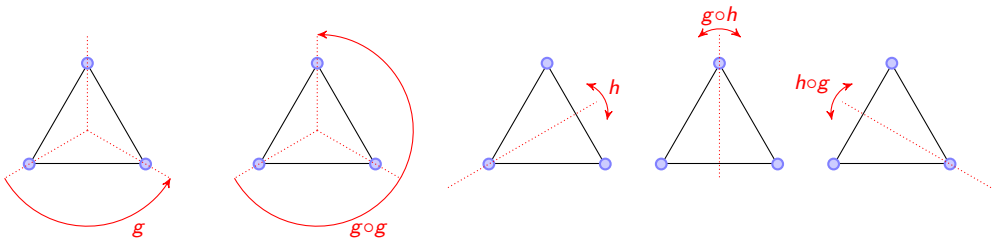
- We will come back to the exercises in Chapter 1 once we have done group actions.
- Chapter 2, Questions 1–2, 4, 6–12 and 14–20 are practise with permutations, and should mainly be revision from Proofs and Problem Solving [L, §20]. It is important that you can do them.

1.1 (Revision of functions) We often take functions for granted, but this is dangerous. Are the following functions?

1. $\mathbb{Z} \to \mathbb{Z}$ sending $a \mapsto a + 2$.
2. $\mathbb{Q} \to \mathbb{Q}$ sending $\frac{a}{b} \mapsto \frac{a}{b} + 2$.
3. $\mathbb{Q} \to \mathbb{Z}$ sending $\frac{a}{b} \mapsto a + b$.
4. $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ sending $(a, b) \mapsto a + 2$.
5. $\mathbb{Q} \times \mathbb{Z} \to \mathbb{Q}$ sending $(\frac{a}{b}, z) \mapsto \frac{a}{bz} + 2$.
6. $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ sending $(\frac{a}{b}, \frac{c}{d}) \mapsto \frac{a}{b} + \frac{c}{d}$.
7. $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ sending $(\frac{a}{b}, \frac{c}{d}) \mapsto \frac{a+c}{b+d}$.

1.2 Find a graph whose only symmetry is the identity.

1.3 Consider the group D_3, which has as elements the identity e and



1. Verify, using a similar argument as in lectures (or otherwise), that these are all the symmetries of the 3-gon.
2. Verify that $h \circ g = g \circ g \circ h$ and so the elements of D_3 are $\{e, g, g \circ g, h, g \circ h, g \circ g \circ h\}$. As in lectures, we drop the $\circ$ and write $D_3 = \{e, g, g^2, h, gh, g^2h\}$.
3. (Cayley Table) Calculate all possible multiplications in D_3. In other words complete the table below, where by definition the entry in the (r, c) position (where r is the row, c the column) is the product $r \circ c$

	e	g	g^2	h	gh	g^2h
e	e	g	g^2			
g	g	g^2	e			
g^2	g^2	e	g			
h						
gh						
g^2h						

1.4 Show that in D_n, the identity e, the $n-1$ rotations and the n reflections are precisely the elements

$$\{e, g, g^2, \dots, g^{n-1}, h, gh, g^2h, \dots, g^{n-1}h\},$$

where g and h were defined in Lecture 2. Then, by modifying your argument to Problem 1.3, show that these are all the symmetries of the n-gon.

1.5 In lectures we showed that we can view the symmetric group S_n as symmetries of the graph with n vertices and no edges. For every $n \geq 2$, produce a *different* graph which also has symmetry group S_n. This is part of the general phenomenon that many different graphs can have the same symmetry group.

1.6 We would like an example of a rotational symmetry of the cube which, if repeated three times, gives the identity. The identity itself has this property. Are there any others?

1.7 How many elements does $\mathrm{GL}(2, \mathbb{Z}_2)$ have? How about $\mathrm{GL}(n, \mathbb{Z}_p)$ with p a prime?

1.8 Are the following operations? For the ones that are operations, do they make the set into a group?

1. $\mathbb{Z}$ with $a * b := a + 2$.
2. $\mathbb{Z}$ with $a * b := a + b$.
3. $\mathbb{Q}$, with $\frac{a}{b} * \frac{c}{d} := \frac{a}{b} + \frac{c}{d}$.
4. $\mathbb{Q}$, with $\frac{a}{b} * \frac{c}{d} := \frac{a+c}{b+d}$.

1.9 Are the following groups?

1. The set $G = \{a + bi \mid a, b \in \mathbb{Z}\}$ with group operation given by addition of complex numbers.
2. The set $G = \{a + bi \mid a, b \in \mathbb{Z}$ and a, b not both zero$\}$ with group operation given by multiplication of complex numbers.
3. The set $G = \{a + bi \mid a, b \in \mathbb{Q}$ and a, b not both zero$\}$ with group operation given by multiplication of complex numbers.
4. The set $K = \{e, x, y, z\}$ with the abelian multiplication defined by

   $$x^2 = y^2 = z^2 = e,\ xy = z,\ yz = x,\ zx = y$$

   and $eg = g$ for all $g \in K$. (Note: you need to check for the existence of inverses and for whether the multiplication is associative: try and organize your reasoning for the latter, exploiting symmetry rather than checking all 64 possibilities.)

1.10 Fix $n \in \mathbb{N}$ and consider multiplication mod n. Let G be the subset of $\{1, 2, \dots, n-1\}$ consisting of all those elements that have a multiplicative inverse (under multiplication mod n). Show that G is a group under multiplication. Describe this group when $n = 12$.

Section 2

Suitable Questions from Jordan and Jordan.

- Chapter 4, Questions 1–11 (all questions).
- Chapter 5, Questions 1–13 (all questions).
- Chapter 6, Questions 1–21 (all questions).

Products

2.1 Give examples of graphs which have symmetry groups $\mathbb{Z}_2$, $S_3 \times \mathbb{Z}_2$ and $S_3 \times D_3$ respectively.

Subgroups

2.2 Suppose that G is a *finite* group and let H be a non-empty subset of G. Show that H is a subgroup of G if and only if $h, k \in H$ implies that $hk \in H$.

2.3 For each of the following, is H a subgroup of G?

1. $G = \mathbb{Z}$ (under addition) and H is all the elements that are multiples of both 3 and 5.
2. $G = \mathbb{Z}$ (under addition) and H is all the elements that are multiples of 3 or multiples of 5.
3. Consider a non-zero vector v in $\mathbb{R}^n$. Take $G = \mathrm{GL}(n, \mathbb{R})$ and
$$H = \{g \in G \mid gv = \lambda v \text{ for some } \lambda \in k\}.$$

2.4 Let $H_1, \ldots, H_k$ be subgroups of G. Prove that their intersection $\bigcap_{j=1,\ldots,k} H_j$ is a subgroup of G.

Cyclic and abelian groups

2.5 Show that if G is cyclic, then G is abelian. Give an example of an abelian group that is not cyclic.

2.6 Let G be cyclic and suppose $G = \langle g \rangle$. Show that if $H \leq G$ and $g \in H$ then $H = G$.

2.7 Find a non-trivial symmetry f of the square (that is, an element of D_4 that is not the identity) that commutes with all the other elements. Which of the groups D_n have such an element?

2.8 Show that if $g^2 = e$ for all $g \in G$, then G is abelian.

2.9 Consider the symmetry groups of the graphs in Workshop 1. Which of them are abelian?

2.10 Let G be the group of 2×2 invertible matrices with entries in $\mathbb{R}$. Let H be the subset consisting of those matrices which are upper-triangular and of determinant 1. Show that H is a subgroup of G. Show that if we replace $\mathbb{R}$ by $\mathbb{Z}_3$, then H is cyclic and hence abelian. Show also that if we replace $\mathbb{R}$ by $\mathbb{Z}_5$ then H is not abelian.

2.11 Show that $\mathbb{Z}_7^*$ (the multiplicative group of nonzero integers mod 7) is a cyclic group.

Order

2.12 Let $x = (g, h) \in G \times H$. Express the order of x in $G \times H$ in terms of the order of g in G and the order of h in H. (A proof is required!)

2.13 In the dihedral group D_6 what are the orders of the various symmetries? (Think carefully and if necessary cut a regular hexagon out of paper and experiment.)

2.14 What is the order of the various elements of the symmetric group S_3?

2.15 Consider $\mathbb{Z}_n$ under addition. Find the orders of all the elements in the cases $n = 3, 4, 5, 6$. What is your guess for the possible orders of elements in $\mathbb{Z}_n$?

2.16 Suppose $o(g) = k$. If $n \in \mathbb{N}$, show that $g^n = e$ if and only if n is a multiple of k.

2.17 Suppose $o(g) = k$. What can you say about the order of g^2?

2.18 Is $o(g) = o(g^{-1})$ always? Give a proof or a counterexample.

Sections 3 and 4

Suitable Questions from Jordan and Jordan.

- Chapter 10, Questions 1, 4–8, and 10–14.
- Chapter 9, Questions 1–4 and 9–10.

Cosets and Lagrange

3.1 Consider the group D_3. Find the left and right cosets of H in D_3 where:

1. $H = \langle g \rangle = \{e, g, g^2\}$.
2. $H = \langle h \rangle = \{e, h\}$

where g and h were defined in Problem 1.3.

3.2 Show that if G is abelian and $H \leq G$, then the left cosets of H in G are the same as the right cosets. Find the cosets in the case where $G = \mathbb{Z}_9$ and $H = \{0, 3, 6\}$.

3.3 Find all the subgroups of D_3.

3.4 Find all the subgroups of $\mathbb{Z}_5$ and $\mathbb{Z}_6$.

3.5 What are all the subgroups of D_4?

Homomorphisms

4.1 Show that exp is a group homomorphism between $\mathbb{R}$ (under addition) and $\mathbb{R}^* := \mathbb{R} - \{0\}$ (under multiplication). What is its kernel and what is its image? Now answer the same question for $\exp : \mathbb{C} \to \mathbb{C}^*$.

4.2 Let p, q be different primes. Show that the only homomorphism $\phi : C_p \to C_q$ is the trivial one (i.e. $\phi(g) = e$ for all g). (Hint: consider kernels and images.)

4.3 Consider the function $\det : \mathrm{GL}(n, k) \to k^*$. Show that it is a group homomorphism. Identify its kernel and image.

Isomorphisms and Products

4.4 Consider the group $\mathbb{C}$ under addition. Show that complex conjugation $\phi : z \to \bar{z}$ is an isomorphism $\mathbb{C} \to \mathbb{C}$.

4.5 Let $a, b \in \mathbb{N}$. True or false: $a!b!$ always divides $(a + b)!$

4.6 Prove that every group G of order 4 is isomorphic to C_4 or $C_2 \times C_2$. (Hint: If G has an element of order 4 then we know the group is isomorphic to C_4. So the only possibility is that every non-identity element has order 2. Call them x, y, z. What are xy and yx equal to?)

4.7 Describe a subgroup of S_7 isomorphic to $S_3 \times S_4$.

4.8 Consider the argument in lectures showing that $D_6 \cong D_3 \times \mathbb{Z}_2$. Does a similar argument apply to D_n, with n *even*, $n \geq 6$? What about D_4?

4.9 If $G \cong H \times \mathbb{Z}_2$, show that G contains an element a of order 2 with the property that $ag = ga$ for all $g \in G$. Deduce (briefly!) that the dihedral group D_{2n+1} (where $n \geq 1$) is not isomorphic to a product $H \times C_2$.

4.10 Show that no two of the three abelian groups of size 8

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_8$$

are isomorphic.

Section 5

Suitable Questions from Jordan and Jordan.

- Chapter 1, Questions 4–10 are good practice for orbits and stabilizers.
- Chapter 7, Questions 1–9 and 13–16 are more practice for orbits and stabilizers.
- Chapter 9, Questions 6–8 for group actions $\leftrightarrow$ homomorphisms.
- Chapter 11, Questions 1–10 mainly involve the orbit–stabilizer theorem.
- Chapter 12, Questions 1–14 are great practice for Pólya counting.

Group actions and Cayley's theorem

5.1 Let a group G act on X. Show that if $y = g \cdot x$ then $x = g^{-1} \cdot y$. (Note: you must argue from the axioms for a group action.)

5.2 Identify the subgroup of S_4 that arises in Cayley's theorem applied to $C_2 \times C_2$. Do the same for C_4.

Faithful and transitive actions

5.3 Show that the symmetry group of any graph always acts faithfully on the set of vertices. Find a graph (with at least two edges) whose symmetry group acts transitively on the set of vertices. Find one whose symmetry group does not act transitively.

5.4 Consider a regular 9-gon with symmetry group D_9. There are three separate equilateral triangles that can be constructed using the nine vertices, and D_9 acts on the set X of the three triangles. Identify the subgroup that acts trivially.

Orbits and stabilizers

5.5 Let G act on X and let $x \in X$. Prove that the stabilizer of x is a subgroup of G.

5.6 Consider the group $G = S_n$ acting on $X = \{1, 2, \ldots, n\}$. Let $x = n$. How many elements does the stabilizer $\mathrm{Stab}_G(x)$ have? To what group is this stabilizer isomorphic?

5.7 Fix a line L through opposite vertices of a cube. Consider the subgroup H of the symmetries of the cube generated by g, where g is a rotation by $1/3$ of a turn about L (this is the element in Problem 1.6). Then H acts on the set of vertices of the cube. Describe the orbits.

5.8 Consider the rotational symmetry group G of the cube acting on the set of vertices of the cube. Describe the stablizer of a particular chosen vertex. How many elements does it have? Now do the same for the action of G on the set of faces and the set of edges.

5.9 For each graph in Workshop 1, let G denote the symmetry group of the graph. Then G acts on the set of vertices. In each case, find how the set of vertices is partitioned into orbits.

5.10 Consider the group $G = \mathrm{GL}(2, \mathbb{Z}_2)$. Then G acts on the vector space $\mathbb{Z}_2^2$ in the usual way by multiplication. Let X be the set of 1-dimensional subspaces of $\mathbb{Z}_2^2$. Then G acts on X. Show that $|G| = 6$, $|X| = 3$, and that every permutation of the elements of X is realized by an element of G. (Hence this is another realization of S_3 acting by permutation on $\{1, 2, 3\}$.)

Orbit–stabilizer theorem

5.11 Check the orbit-stabilizer theorem for the case of the group S_n acting on a set of n objects by permuting them.

5.12 The rotational symmetry group G of a dodecahedron acts transitively on the set V of its 20 vertices. Pick $v \in V$. How many elements are in the stabilizer of v? (you may have to make the model of the dodecahedron and play with it) Deduce the order of G. Using a similar method, deduce the order of the group of rotational symmetries of the octahedron.

5.13 By Problem 5.12 you should know that there are 24 elements in the group of rotational symmetries of the octahedron. What are they? (you just have to describe 24 distinct symmetries, then automatically you have them all.)

Pólya counting

5.14 Dice have the numbers $1, 2, 3, 4, 5, 6$ on the faces of a cube in such a way that opposite faces add up to 7. How many different dice are there? (Two dice are the same if they differ by a rotational symmetry of the cube. There are 24 such symmetries.) You can solve this by "pure thought" only because the numbers involved are small; try to find a group-theoretic answer.

5.15 How many ways are there of colouring the vertices of a 6-gon with two colours, where two colourings are regarded as the same if they differ by an element of D_6? (Be careful to think about the different sorts of rotation and reflection. It is more complicated than the 5-gon example in lectures.)

Challenge Question

5.16 (Sylow's 1st Theorem) Let G be a finite group and let p be a prime factor of $|G|$, and suppose that $k \in \mathbb{N}$ is largest such that p^k divides $|G|$. Then G contains a subgroup H such that $|H| = p^k$. Prove this in stages:

1. Let $\mathcal{S} := \{U \subseteq G : \ |U| = p^k\}$, i.e. the set of all subsets of G with p^k elements. Show that G acts on $\mathcal{S}$ via the rule $g \cdot U := gU$.
2. Argue that p does not divide $|\mathcal{S}|$.
3. By 1, $\mathcal{S}$ is partitioned into orbits. Using 2, deduce that there exists an orbit $\mathcal{A}$ such that p does not divide $|\mathcal{A}|$.
4. Pick an element $V \in \mathcal{A}$, and consider $H := \mathrm{Stab}_G(V)$. Why is H a subgroup?
5. Argue that p^k divides $|H|$ by using the orbit-stabilizer theorem.
6. Argue directly that $|H| \leq p^k$.
7. By combining your answer to 4, 5 and 6, prove the 1st Sylow Theorem.

Sections 6 and 7

Suitable Questions from Jordan and Jordan.

- Chapter 13, Q1–21 are good practice for conjugates, centralizers and centres.
- Chapter 14, Q1–17 for Cauchy's Theorem, product groups and applications.
- Chapter 15, Q1–18 for kernels and normal subgroups.

Symmetric and Alternating Groups

6.1 Prove that if σ_1 and σ_2 are disjoint cycles, then $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

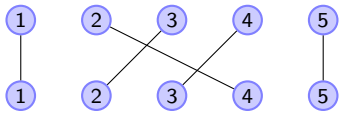
6.2 Show that the number of elements of S_n of cycle type $1^{m_1}, 2^{m_2}, \dots, n^{m_n}$ is

$$\frac{n!}{m_1! \dots m_n! 1^{m_1} 2^{m_2} \dots n^{m_n}}.$$

6.3 Let $\sigma \in S_n$ have cycle type $l_1, \dots, l_k$. What is the order of σ? What are the possible orders of elements in S_7?

6.4 Let $\sigma \in S_n$ and let $H := \langle \sigma \rangle$ act on $\{1, 2, \dots, n\}$ in the obvious way. Convince yourself that the cycle type of σ is the list of the sizes of all the orbits of this action.

6.5 Let $\sigma \in S_n$. Another notation for writing σ is the following: write the numbers $1, \dots, n$ in two rows, one above the other. Then for every number i in the top row, draw a line between i (in the top row) and $\sigma(i)$ on the bottom row, for example



represents $1 \mapsto 1$, $2 \mapsto 4$, $3 \mapsto 2$, $4 \mapsto 3$ and $5 \mapsto 5$. From this picture, can you tell whether a permutation is odd or even? Also, how do you compose permutations using this picture?

6.6 Prove that A_4 is not isomorphic to D_6.

Conjugate elements, centres and centralizers

6.7 Let $g \in G$. Show that $\langle g \rangle \leq C(g)$.

6.8 Let $g \in G$. Prove directly (i.e. without using general properties of group actions) that $C(g) \leq G$.

6.9 Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \in G = \mathrm{GL}(2, \mathbb{Z}_3)$. Show that $|C(A)| = 4$. What is $|G|$? How many conjugates does A have in G?

6.10 Let $\phi : G \to \mathrm{GL}(n, k)$ be a group homomorphism. Show that the function $f : G \to k$ defined by $f(g) = \mathrm{Trace}\, \phi(g)$ is constant on every conjugacy class of G.

6.11 Consider D_6, the symmetries of a regular hexagon. Let $H \leq G$ be the subgroup consisting of the identity and the five nontrivial rotations. Let g denote a rotation by $1/6$ of a turn. Show that $H \leq C(g)$. Find an element in D_6 that does not commute with g and hence use Lagrange's theorem to deduce that $C(g) = H$. From this, deduce that g is conjugate to only one other element of D_6, and find that element.

6.12 Let k be a field, $n \in \mathbb{N}$. Show that the centre of $\mathrm{GL}(n, k)$ is $\{\lambda \mathbb{I} \mid \lambda \in k^*\}$. (It is clear that the centre contains at least these matrices. The content in the question is that it does not contain other things.)

6.13 What is the centre of the dihedral group D_n? (Hint: consider n odd and even separately.)

Conjugacy classes

6.14 Find the conjugacy classes in D_4. (If necessary, cut out a square from paper, label the corners and play with it.)

6.15 Let $G = H \times K$. Show that (h, k) is conjugate to (h', k') in G if and only if h and h' are conjugate in H, and k and k' are conjugate in K. This shows that every conjugacy class in G is of the form $C \times D$ where C is a conjugacy class in H, and D is a conjugacy class in K. Hence write down the class equation for $C_2 \times S_3$.

6.16 Write down the class equation for D_4. (You should have done most of the work in Problem 6.14.)

6.17 Let p be a prime. You know that every group of order p is cyclic, and thus abelian (by Problem 2.5). You also know (from lectures) that every group of order p^2 is abelian. Is the same true for p^3, i.e. is every group of order p^3 abelian?

6.18 Consider the cycles $c = (125)$ and $d = (234)$ in S_5. Find $g \in S_5$ such that $d = gcg^{-1}$. How many such g are there?

6.19 S_4 has five conjugacy classes. Find them, and the number of elements in each, and hence write down the class equation for S_4.

6.20 Show that $(12)(34)$ together with its conjugates and the identity form a subgroup of S_4 isomorphic to $C_2 \times C_2$.

Normal subgroups

6.21 Let $N \leq G$. Prove that the following are equivalent:

1. N is normal in G.
2. $gNg^{-1} = N$ for all $g \in G$.
3. $gN = Ng$ for all $g \in G$.

6.22 Prove that if $\phi : G \to H$ is a group homomorphism, then $\operatorname{Ker} \phi$ is a normal subgroup of G.

6.23 Find all the normal subgroups of D_4. (There are six in total!) One of them, which we will call N, has order 2. To what familiar group is the quotient D_4/N isomorphic?

6.24 Show that the intersection of two normal subgroups is a normal subgroup.

6.25 Show that $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of S_4.

6.26 Show that $\{e\}$, V_4 (in the previous exercise), A_4 and S_4 are the only normal subgroups of S_4. (Hint: a subgroup is normal iff it is a union of conjugacy classes. Use the class equation and Lagrange's Theorem.)

6.27 (harder) The aim of this exercise is to show that A_5 has no normal subgroups other than $\{e\}$ and A_5 itself. (Groups with this property are called *simple*. They are fundamental building blocks because if $N \trianglelefteq G$ is a normal subgroup one can regard G as being in some sense built from the smaller groups N and G/N).

1. Show that A_5 consists of: the identity; 15 elements of cycle-type 2,2; 20 3-cycles; 24 5-cycles.
2. We know that all 5-cycles are conjugate in S_5, however this may not be true in A_5 because the element that does the conjugation in S_5 might be odd (and so doesn't belong to A_5). Now, we know (by orbit-stabilizer) that the number of elements in the conjugacy class of $g \in A_5$ is equal to $\frac{|A_5|}{|C_{A_5}(g)|}$. Show that the centralizer of a 5-cycle in A_5 is the cyclic group that it generates and hence conclude that the 5-cycles constitute 2 size-12 conjugacy classes.
3. Deduce similarly that (in A_5) the elements of cycle-type 2,2 form a conjugacy class of size 15 and the 3-cycles form a conjugacy class of size 20.
4. Use the characterization of a normal subgroup as a subgroup that is a union of conjugacy classes, and Lagrange's theorem, to show that A_5 is simple.

Quotient groups

6.28 Show that D_n has a normal subgroup isomorphic to C_n, with $D_n/C_n \cong C_2$.

6.29 Prove that the map $\bar{\phi} : G \to G/N$ given by $\bar{\phi}(g) = gN$ is a group homomorphism.

6.30 Show that every homomorphism $\phi : \mathbb{Z} \to G$ (regarding $\mathbb{Z}$ as a group under addition) is of the form $\phi : k \mapsto g^k$ for some $g \in G$. (Hint: consider $\phi(1)$.) Describe the kernel and image of such a ϕ.

6.31 How can one understand the addition of angles in terms of a quotient group?

6.32 Determine whether the following claims are TRUE or FALSE. If they are true give a proof, whereas if they are false give a counterexample.

1. Every group of order six is abelian.
2. Every group of order fourteen is abelian.
3. If G is non-abelian, then $\{g \in G \mid gh = hg \text{ for all } h \in G\} = \{e\}$.
4. Every normal subgroup of a group G is the kernel of some group homomorphism.
5. Let $n \geq 2$, then the group $\mathrm{GL}(n, \mathbb{R})$ has no normal subgroups other than $\{e\}$ and $\mathrm{GL}(n, \mathbb{R})$.