MATH10021 Algebra

INTRODUCTION

TO

GROUP THEORY

Michael Wemyss

✪

2012/13

Dr. Michael Wemyss
Office 5602
m.wemyss@ed.ac.uk

Throughout the term, all course information (including exercise sheets, workshop sheets and problems for handin) will be available at

http://www.maths.ed.ac.uk/∼mwemyss/teaching/3alg2013.html

Suggested problems will be assigned every Thursday in class, and their numbers will be posted online on the above webpage.

Contents

1. **Groups and Examples**

1.1. **Basics**

1.1.1. *Definition.* A *group* is a non-empty set G together with a rule that assigns to each pair g, h of elements of G an element $g * h$ such that

- $g * h \in G$. We say that G is *closed* under $*$.
- $g * (h * k) = (g * h) * k$ for all $g, h, k \in G$. We say that $*$ is associative.
- There exists an *identity element* $e \in G$ such $e * g = g * e = g$ for all $g \in G$.
- Every element $g \in G$ has an *inverse* g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

1.2. **First examples of groups**

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. You already know lots of examples of groups.

1. The integers $\mathbb{Z}$ under addition is a group with $g * h := g + h$. The identity is 0 and the inverse of x is $-x$.
   - Similarly with $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ (or indeed any other field) under addition.
2. For all $n \in \mathbb{N}$, the *integers mod n*, which we denote $\mathbb{Z}_n$, forms a group under addition. The the identity is 0, and the inverse of x is $-x$. (Strictly of course elements of $\mathbb{Z}_n$ are equivalence classes, but we are expressing things in terms of representatives.)
3. 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.
4. 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 field under multiplication with identity 1 and inverse $1/x$.
5. Let k be a field and choose $n \in N$. Then $G = \mathrm{GL}(n, k)$ is defined to be the set of all invertible $n \times n$ matrices with entries in k. This is a group with $g * h$ given by matrix multiplication. (One can regard it as the symmetries of the vector space k^n — see §1.8.1 later)

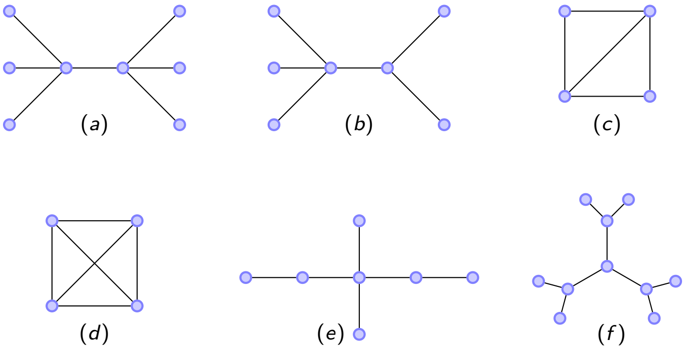
1.3. **Symmetries give groups**

Roughly speaking, a *symmetry* of an object is a bijection (i.e. one-to-one correspondence) from the object to itself that preserves its structure. This is not a mathematical definition, it just gives you the theme of the next few sections. I will make this more precise in some examples (see §1.4, §1.5, §1.6 and §1.7). As a slogan, 'symmetries give groups'.

1.4. **Symmetries of graphs**

1.4.1. *Definition.* 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.

1.4.2. *Examples.*



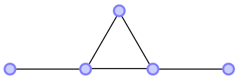
(*a*) (*b*) (*c*)

(*d*) (*e*) (*f*)

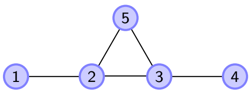
1.4.3. *Definition.* A *symmetry* of a graph is a permutation of the vertices that preserves the edges. More precisely, let V denote the set of vertices of a graph. Then a symmetry is a bijection $f : V \to V$ such that $f(v_1)$ and $f(v_2)$ are joined by an edge if and only if v_1 and v_2 are joined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

Note that symmetries must preserve the valency of a vertex, hence if v_1 has valency three, then $f(v_1)$ must also have valency three.

1.4.4. *Example.* Consider the graph



For convenience, number the vertices

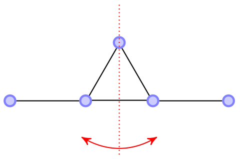


so V, the set of vertices, is $V = \{1, 2, 3, 4, 5\}$. Let $f : V \to V$ be a symmetry of the graph. Since 5 is the only vertex with valency two, $f(5) = 5$. Since 2 and 3 are the only vertices that have valency three, necessarily $f(2) = 2$ or 3, and $f(3) = 3$ or 2.

Suppose that $f(2) = 2$. Since f is a bijection, $f(3) \neq 2$ and so $f(3) = 3$. Thus 2, 3 and 5 are all fixed by f. This then forces $f(1) = 1$ (since $f(1)$ must be joined to $f(2) = 2$, and it can't be 5 since $f(5) = 5$) and similarly $f(4) = 4$. This means that f is the identity.

On the other hand, suppose $f(2) = 3$. This forces $f(3) = 2$. We already know that $f(5) = 5$. Since 1 has valency one, either $f(1) = 1$ or 4. Since $f(1)$ must be joined to $f(2) = 3$, necessarily $f(1) = 4$. Similarly $f(4) = 1$.

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



1.4.5. *Theorem.* The symmetries of a graph forms a group.

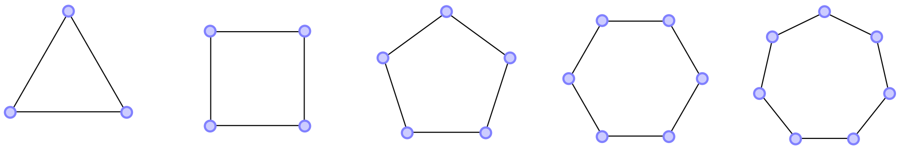
Proof. If $f : V \to V$ and $g : V \to V$ we define the group operation $f * g$ to be their composition (as maps), so $f * g := f \circ g$, i.e. *do* g *first, then* f. The composition of symmetries is clearly a symmetry, so the operation is closed. Since the composition of maps is associative

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

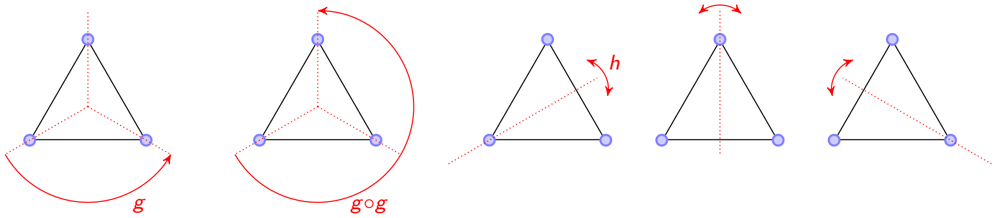
for all symmetries f, g, h. The identity map e which sends every vertex to itself is a symmetry, and obviously $e \circ f = f \circ e = f$ for all symmetries f. Lastly, if $f : V \to V$ is a symmetry then it is bijective, so it inverse f^{-1} exists and is also a symmetry. It is characterized by $f \circ f^{-1} = f^{-1} \circ f = e$. □

1.5. **Symmetries of regular *n*-gons**

We view the *n*-gon as a graph, and apply the last section. In particular, by §1.4.5 the symmetries of an *n*-gon form a group. Here we investigate these in more detail.

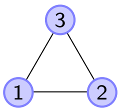


1.5.1. *Symmetries of an equilateral triangle.* Consider a 3-gon, i.e. an equilateral triangle. There are precisely six symmetries of the 3-gon:

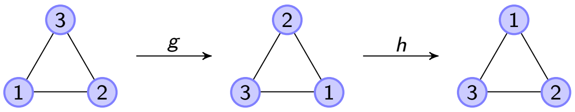


- e the identity (not drawn above).
- Rotation anticlockwise by $2\pi/3$ (which we call g), and rotation anticlockwise by $4\pi/3$. The latter is drawn in the second diagram, and corresponds to performing g twice.
- The three reflections in the lines through the three vertices. These are drawn in the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

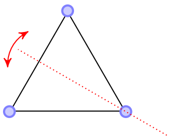
The proof that these six symmetries are all the symmetries of the 3-gon is rather similar to the proof in §1.4.4 (see Problem 1.2). Now if we label the vertices as



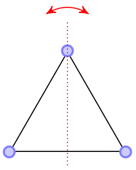
then



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



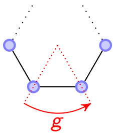
Similarly $g \circ h$ is equal to



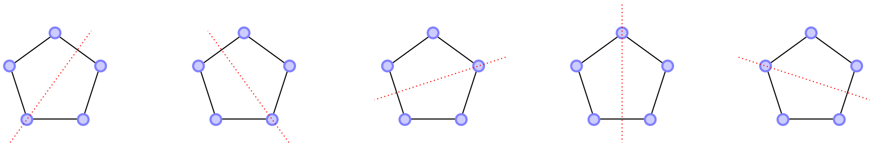
and so $D_3 = \{e, g, g \circ g, h, g \circ h, h \circ g\}$. As a piece of notation we usually drop the symbol $\circ$ and so $D_3 = \{e, g, g^2, h, gh, hg\}$. See also Problem 1.2.

1.5.2. *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:

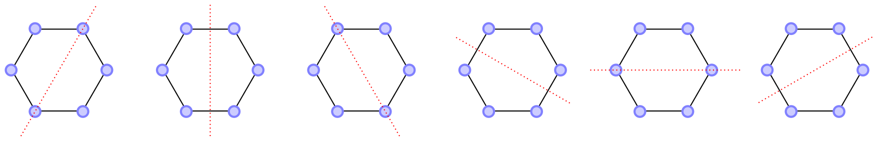
- The identity e.
- The $n-1$ rotations through angles $k2\pi/n$ ($k = 1, \dots, n-1$) anticlockwise. If we denote g to be the rotation anticlockwise through $2\pi/n$, i.e.



  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

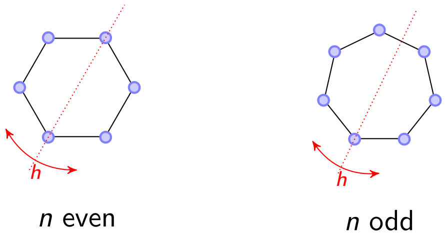


whereas if $n = 6$ there are six reflections



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.



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 1.3.

1.6. Symmetries of finite sets (=the symmetric group)

1.6.1. *Symmetric groups.* A symmetry of a set X of n objects is a *permutation* (i.e. a bijection $X \to X$). There are $n!$ in total and these form the *symmetric group* S_n.

1.6.2. *Remarks.*

1. This is really a special case of §1.4, since S_n is the group of symmetries of the graph with n vertices and no edges. Thus we already know (by §1.4.5) that S_n is a group.
2. When dealing with the symmetric group S_n, we always 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. One notation for doing this is illustrated in §1.6.3 below; see §6 for other methods.

1.6.3. *The symmetric group S_3.* Let $X = \{1, 2, 3\}$. Then S_3 has six elements:

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

The notation here is that the map sends the entry in the top row to the entry below it. Thus the first one is the identity and the last sends $1 \mapsto 3, 2 \mapsto 1$ and $3 \mapsto 2$.

1.6.4. *Initial remark.* Although D_3 and S_3 have different definitions it turns out (see §3.1.4) that they are really "the same" group. The technical term is *isomorphic* — we will give a more precise definition later.

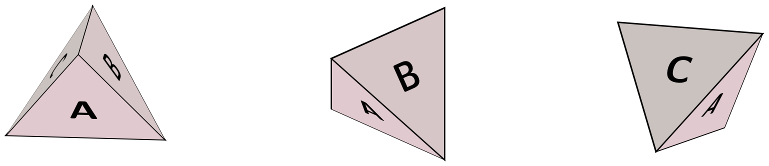
We will study symmetric groups more in §6.

1.7. (Rotational) Symmetries of regular solids

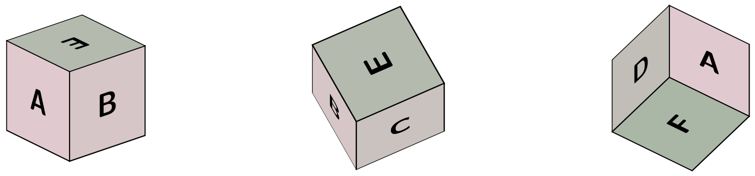
1.7.1. *Platonic solids.* There are five platonic solids (convex bodies whose faces are all similar regular polygons and such that every vertex is identical).

	Faces	Edges	Vertices	Faces per vertex	Rot. syms
tetrahedron	4 triangles	6	4	3	12
hexahedron	6 squares	12	8	3	24
octahedron	8 triangles	12	6	4	24
dodecahedron	12 pentagons	30	20	3	60
icosahedron	20 triangles	30	12	5	60

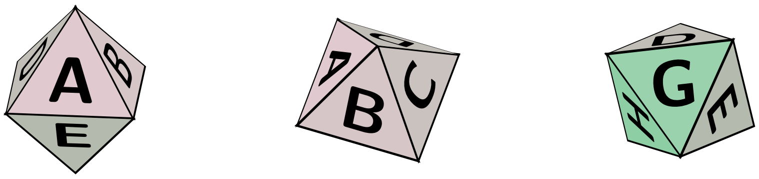
We will consider their groups of *rotational symmetries*. These are rotations (necessarily about the centres of faces, vertices and edges) that leave the solid fixed.
The tetrahedron:



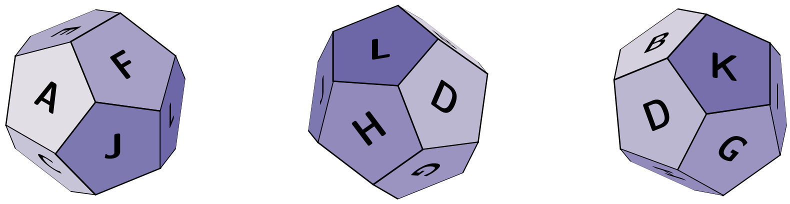
The hexahedron(=the cube):



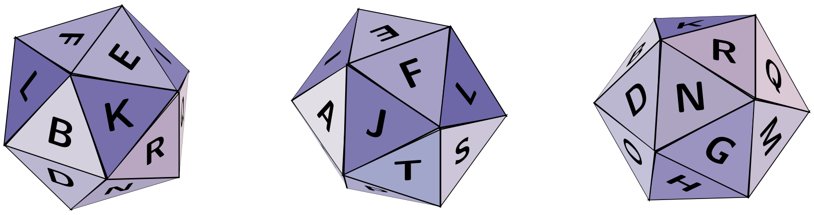
The octahedron:



The dodecahedron:



The icosahedron:



These solids have interesting symmetries, but it is much harder to prove how many there are by arguing as in §1.4. I will come back to these examples after we know some more theory. You can make your own dodecahedron 2013 calendar at

http://www.maths.ed.ac.uk/∼mwemyss/teaching/Calendar2013.pdf,

which will be turn out to be useful later when you try to solve problems.

1.8. **Symmetries of vector spaces**

Let V be a vector space of dimension n over a field k. Going with our guiding principle in §1.3, a symmetry of V should be a bijection $V \to V$ that preserves the structure of V. In other words, it should preserve the linear structure, so it should be a linear map. Thus we define:

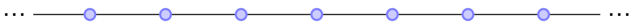
1.8.1. *Definition.* A symmetry of a vector space V is a linear isomorphism $V \to V$.

If we choose a basis for V then such an isomorphism is described by an $n \times n$ invertible matrix with entries in k. So (after that choice of basis) we can identify the symmetries of a vector space with

$$\mathrm{GL}(n,k) := \{\ n \times n \text{ invertible matrices with entries in } k\}.$$

1.9. **A 1-dimensional lattice**

1.9.1. *Definition.* Consider the subset $L = \{n \mid n \in \mathbb{Z}\}$ of the real line $\mathbb{R}$. Thinking of L as an infinite pattern of dots,

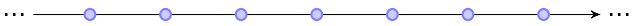


there are two types of symmetry:

- For each $k \in \mathbb{Z}$, a *translation* $T_k : n \mapsto n + k$.
- For each $l \in \mathbb{Z}$ there is the reflection $M_l : n \mapsto l - n$. (This reflects in the point $l/2 \in \mathbb{R}$.)

1.9.2. *Remarks.* What we have here is the symmetries of an infinite graph. The identity symmetry e in the description above is the "trivial translation" T_0.

1.9.3. *Orientation.* We could alternatively view the real line $\mathbb{R}$ as oriented



Note that translations maintain the orientation of the line, whilst the reflections reverse it. If we regard the line as oriented, then only the translations are symmetries.

2. **First Properties of Groups**

From now on we assume only the group axioms.

2.1. **First basic properties**

2.1.1. *Lemma.* Let $g, h \in G$ be given. Then there is one and only one element $k \in G$ such that $k * g = h$. Similarly, there is one and only one $l \in G$ such that $g * l = h$.

Proof. 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. The case for $g * l = h$ is similar. □

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

2.1.3. *Corollaries.*

1. In a group you can always cancel: if $g * s = g * t$ then $s = t$. Similarly, if $s * g = t * g$ then $s = t$.

   Proof. Let $h := g * s$. Then also $h = g * t$, so by uniqueness in §2.1.1, $s = t$. □

2. Fix $g \in G$. Then left multiplication by g defines a map $L_g : G \to G$ where $L_g(k) = g * k$. The map L_g is a bijection (i.e. it permutes the elements of G). Similarly for right-multiplication.

   Proof. Let $h \in G$, then by §2.1.1 there is one element k for which $g * k = h$, and so L_g is surjective. Since there is only one such k (also by §2.1.1), L_g is injective. □

3. 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 $(g^{-1})^{-1} = g$.

   Proof. 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 $(g^{-1})^{-1} = g$. □

4. A group has only one identity: if $g * h = h$ (even just for one particular h) then $g = e$.

Proof. We have $g * h = h = e * h$, so by cancelling h on the right (using part 1), $g = e$. □

2.2. Commutativity

If G is a group and $g, h \in G$, if $g * h = h * g$ 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.

2.2.1. *Remark.* It is very important to understand that not all groups are abelian.

2.2.2. *Examples.*

1. Any field, or indeed any vector space, is an abelian group under addition.
2. $\mathbb{Z}_n$ 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 §1.5.1).
5. In §1.9 the group of orientation–preserving symmetries of L is an example of an abelian group, since $T_k \circ T_l = T_{k+l} = T_l \circ T_k$ for all $k, l \in \mathbb{Z}$.
6. In §1.9 the group of all symmetries of L is an example of a group which is not abelian, since $M_0 \circ T_1 \neq T_1 \circ M_0$ (check!).

2.3. Some basic definitions

2.3.1. *Definition.* (order of a group) A *finite group* 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.)

2.3.2. *Definition.* (order of an element) Let $g \in G$. Then the *order* $o(g)$ of g is the *l*east natural number n such that $\underbrace{g * \dots * g}_{n} = e$. If no such n exists, we say that g has infinite order.

2.3.3. *Examples.*

1. See Problems 2.3 – 2.8 for many examples of finite order.
2. In §1.9, if $k \neq 0$ then the elements T_k are examples of elements of infinite order. There is no $n \in \mathbb{N}$ such that $\underbrace{T_k \circ \dots \circ T_k}_{n}$ equals the identity.

2.3.4. **Important notation.**

- When dealing with a general group G, we will write gh for $g * h$, the identity as e (or 1), and the inverse of g as g^{-1}.

We do this since it is tedious to keep on writing $*$. However, this can create confusion. For example, when the group is $\mathbb{Z}_n$ (under addition),

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

Hence, when you are dealing with groups under addition, it is helpful to keep the $*$ notation in (see for example §2.9.3 later).

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

Proof. Let $g \in G$. Consider the infinite sequence $g, g^2, g^3, \dots$. 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), $g^{m-n} = e$. □

2.3.6. *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 §2.3.5 there exists $t \in \mathbb{N}$ such that $g^t = e$. Applying g^{-1} to both sides gives $g^{t-1} = g^{-1}$. □

2.4. **Subgroups**

2.4.1. *Definition.* A subset $H \subseteq G$ is a *subgroup* of G if

- H is not empty.
- If $h, k \in H$ then $hk \in H$
- If $h \in H$ then $h^{-1} \in H$.

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

2.4.2. *Notes.*

1. If H is any subgroup, the axioms ensure that H is a group in its own right. Make sure that you can prove this.
2. If G is finite, then there is a slightly easier test for a subgroup. See Problem 2.12.

2.4.3. *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 k be a field and let $G = \mathrm{GL}(2, k)$. Let H be all the upper-triangular elements of G. Then $H < G$.

2.5. **Products**

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

2.5.1. *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. Each axiom for $G \times H$ follows trivially from the same axiom for G and H. □

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

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

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

2.5.4. *Examples.*

1. You already know examples of products. Let k be a field regarded as an abelian group under addition. Then the vector space k^2, regarded as a group under addition, is just $k \times k$ defined above.
2. Consider a set S of four identical red balls and three identical blue balls. A symmetry of S is then any bijection $S \to S$ such that red balls are taken to red balls, and blue balls are taken to blue ones. The group of symmetries is thus $S_4 \times S_3$ since a symmetry is specified by choosing a permutation of four objects and a permutation of three objects.

2.5.5. *Definition.* The product of more than two groups can also be regarded as a group, in the obvious way.

We will come back to products in §3.2.

2.6. **Cyclic subgroups**

The easiest type of subgroup.

2.6.1. *Definition.* If G is a group, $g \in G$ and $k \in \mathbb{Z}$, define

$$g^k := \begin{cases} \overbrace{g \dots g}^{k} & \text{if } k > 0 \\ e & \text{if } k = 0 \\ \underbrace{g^{-1} \dots g^{-1}}_{-k} & \text{if } k < 0 \end{cases}$$

and further define

$$\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\} = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}.$$

If G is finite, then $\langle g \rangle$ (being a subset of G) is finite, and we can think of $\langle g \rangle$ as

$$\langle g \rangle = \{e, g, \dots, g^{o(g)-1}\}$$

by §2.3.5 and §2.3.6.

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

Proof. Just check the axioms. Make sure that you can do this. 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 is cyclic. One possible generator is rotation by $2\pi/n$, (the element in §1.5.2 which was denoted by g). There are other possible generators too, for example g^{-1}.
4. In $\mathbb{R}$ under addition, $\langle 1 \rangle = \mathbb{Z}$ which is an example of an infinite cyclic subgroup.

2.7. **Generators**

Cyclic groups are, by definition, generated by a single element. We now generalize this to more than one element.

2.7.1. *Definition.* Let $S \subseteq G$ be a nonempty subset. Define $\langle S \rangle$ to be the set of all finite products of elements of S and their inverses. More precisely,

$$\langle S \rangle = \{g_1 g_2 \dots g_k \mid g_j \in S \text{ or } g_j^{-1} \in S, k \in \mathbb{N}\}.$$

For example, if $S = \{g, h\}$ then $gh^{-1}gghg^{-1}$ and $h^{-1}g^{-1}h$ are members of $\langle S \rangle$.

2.7.2. *Theorem.* Let $S \subseteq G$ be nonempty. Then

1. $\langle S \rangle$ is a subgroup of G
2. $\langle S \rangle$ is the smallest subgroup of G that contains S (in the sense that if $H \leq G$ is a subgroup and $S \subseteq H$, then $\langle S \rangle \leq H$).

Proof. 1. Since $S \neq \emptyset$, $\langle S \rangle \neq \emptyset$. If $g_1 \dots g_k \in \langle S \rangle$ and $g_1' \dots g_k' \in \langle S \rangle$, then their product $g_1 \dots g_k g_1' \dots g_k' \in \langle S \rangle$. Finally, if $g_1 \dots g_k \in \langle S \rangle$ then certainly $g_k^{-1} \dots g_1^{-1} \in \langle S \rangle$ and further

$$(g_1 \dots g_k)(g_k^{-1} \dots g_1^{-1}) = e = (g_k^{-1} \dots g_1^{-1})(g_1 \dots g_k).$$

2. It is clear from the definition that $S \subseteq \langle S \rangle$, so $\langle S \rangle$ is a subgroup of G containing S. Now let $H \leq G$ such that $S \subseteq H$. Since H is closed under multiplication and inverses, certainly every member of $\langle S \rangle$ is contained in H, so $\langle S \rangle \subseteq H$. □

2.7.3. *Definition.* If $\langle S \rangle = G$ we say that the elements of S *generate* G and refer to S as a *set of generators*.

2.7.4. *Theorem.* If G is a finite group and $S \subseteq G$, then

$$\langle S\rangle = \{g_1 g_2 \dots g_k \,|\, g_j \in S, k \in \mathbb{N}\}.$$

(Proof: §2.3.6.)

2.7.5. *Example.* Consider the group D_n, and let $S = \{g, h\}$ where g and h are defined in §1.5.2. Since $D_n = \{e, g, \dots, g^{n-1}, h, gh, \dots, g^{n-1}h\}$ and each of these elements belongs to $\langle S\rangle$, it follows that $D_n \subseteq \langle S\rangle$. But $\langle S\rangle$ is a subgroup of D_n and so the reverse inclusion also holds, hence $D_n = \langle g, h\rangle$.

2.8. **Generators and relations**

2.8.1. *Motivation.* Consider again the group D_n, with g and h as defined in §1.5.2. Then clearly $g^n = e$ and $h^2 = e$. Furthermore, $hg = g^{-1}h$ (this is similar to Problem 1.2 part 2). Thus we have

$$g^n = e, \quad h^2 = e, \quad hg = g^{-1}h.$$

These *relations* between the *generators* g, h tell us everything about the group, as we will now see.

A *word* is any string of generators such as, for example, *gghgghhhggh*. Using the last relation we can always move all the h's to the right of this string and having done so we can use the first two relations so as to obtain one of the following words:

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

We know that these are all the elements of D_n. We summarize this in the presentation

$$D_n = \langle g, h \mid g^n = 1, h^2 = 1, hg = g^{-1}h\rangle.$$

2.8.2. *Note.* Presentations are useful for calculating messy products that would take a long time to do pictorially. For example, we can compute a product in D_4 as follows:

$$(g^3h)(g^2h) = ggghggh = gghgh = ghh = g.$$

This gives an alternative way to tackle Problem 1.2 (part 3), which involves much less pain.

2.9. **Lagrange's theorem**

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

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

and similarly for other obvious variants.

2.9.2. *Definition.* 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 $g \in G$.

2.9.3. *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 $g_1 \neq g_2$.

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

As above in §2.9.3, usually the number of members of G/H (which we denote by $|G/H|$) is less than $|G|$. See §2.9.8 for the precise answer later.

2.9.5. *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 $h_1 = h_2$. □

2.9.6. *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) $g_1 H = g_2 H$.
   (b) there exists $h \in H$ such that $g_2 = g_1 h$.
   (c) $g_2 \in g_1 H$.
3. For a fixed $g \in G$, the number of $g_1 \in G$ such that $gH = g_1 H$ is equal to $|H|$.
4. For $g_1, g_2 \in G$, define $g_1 \sim g_2$ if and only if $g_1 H = g_2 H$. 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) ⇒ (c) Suppose that $g_1 H = g_2 H$, then $g_2 = g_2 e \in g_2 H = g_1 H$.
(c) ⇒ (b) This is true by definition of $g_1 H$.
(b) ⇒ (a) Suppose that there exists $h \in H$ such that $g_2 = g_1 h$, then

$$g_2 H = (g_1 h)H = g_1(hH) = g_1 H$$

where the last equality is part 1.
3. By part 2, $gH = g_1 H$ if and only if $g_1 \in gH$. Since $|gH| = |H|$ (by §2.9.5), there are precisely $|H|$ possibilities.
4. Is easy to verify using part 2. Make sure that you can do this. □

2.9.7. *Corollaries.* 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 §2.9.6 there is an equivalence relation $\sim$ defined on G. Thus G is partitioned into a (disjoint union) of the equivalence classes, so

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

By §2.9.6 part 3, for every $g \in G$ the equivalence class containing g has precisely $|H|$ members. Hence every equivalence class has precisely $|H|$ members, and so

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

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, we showed that the number of conjugacy classes was $\frac{|G|}{|H|}$. This then implies:

2.9.8. *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 $\frac{|G|}{|H|}$. □

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

2.10. **Right cosets**

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

2.10.2. *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, §2.9.8 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 2.22).
3. Special things happen when the left cosets equal the right cosets (see for example §3.3.2 and §3.4.2 later).

2.11. First applications of Lagrange

2.11.1. *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 $H = G$. □

2.11.2. *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 2.11.1) and hence abelian (by Problem 2.17). 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 2.17). Therefore we can assume that G has no element of order four. Only the identity has order one, so by Lagrange (2.9.7 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 2.10). □

We already know that the dihedral group D_3 has six elements (since $|D_n| = 2n$ by §1.5.2), and further D_3 is non-abelian (by 2.2.2 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.

3. Fundamental Properties of Groups

3.1. Homomorphisms

3.1.1. *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.)

3.1.2. *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.

3.1.3. *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'.

3.1.4. *Examples.*

1. Consider $\mathbb{R}$ under addition and $\mathbb{R}_+^*$ (the group of positive real numbers) under multiplication. The map $\exp : \mathbb{R} \to \mathbb{R}_+^*$ 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 §2.11.1 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 1.2 and check where every product gets sent to), hence it is an isomorphism, so $D_3 \cong S_3$.

3.1.5. *Lemma.* Let $\phi : G \to H$ be a group homomorphism. Then

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

2. The *image* of ϕ, defined by
$$\operatorname{im}\phi := \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}$$
is a subgroup of H.
3. We define the *kernel* of ϕ by
$$\operatorname{Ker}\phi := \{g \in G \mid \phi(g) = e_H\}.$$
Then $\phi : G \to H$ is injective if and only if $\ker\phi = \{e_G\}$.
4. If $\phi : G \to H$ is injective, then ϕ gives an isomorphism $G \cong \operatorname{im}\phi$.

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. We have $e \in \operatorname{Im}\phi$ by part 1, so $\operatorname{Im}\phi \neq \emptyset$. Further, $\operatorname{Im}\phi$ is closed under multiplication since ϕ is a group homomorphism. Lastly, by part 1 $\operatorname{Im}\phi$ is closed under inverses.
3 and 4 are important exercises, see Problem 3.1. □

3.2. More examples of isomorphic groups

We begin in §3.2.2 with an abstract isomorphism, then show in Examples §3.2.5 and §3.2.6 that this gives us very concrete examples of some isomorphic groups.

3.2.1. *Definition.* (reminder) If S and T are subsets of G, then we define
$$ST := \{st \,|\, s \in S,\ t \in T\}.$$

3.2.2. *Theorem.* 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.

3.2.3. *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

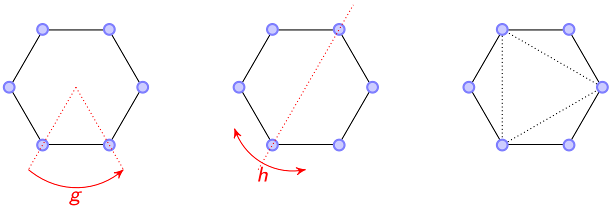
$$\phi((h,k) * (h',k')) = \phi(hh', kk') = hh'kk' = (hk)(h'k') = \phi(h,k)\phi(h',k')$$

(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. □

3.2.4. *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 §3.2.2 (part 1), this is obvious (recall §2.5.3). □

3.2.5. *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 §3.2.2 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 $D_6 \cong D_3 \times \mathbb{Z}_2$.

3.2.6. *More Examples.*

1. The example considered in §2.5.4 can also be analysed as follows. The subgroup H of S_7 that leaves the three blue balls fixed is isomorphic to S_4, and the subgroup K of S_7 that leaves the four red balls fixed is isomorphic to S_3. These subgroups intersect trivially and their elements commute. So HK is a subgroup of S_7 isomorphic to $S_4 \times S_3$.
2. The group G of symmetries of the graph (e) in §1.4.2 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 $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
3. Similarly, in the graph (b) in §1.4.2 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 $G \cong S_3 \times \mathbb{Z}_2$.

3.3. **Normal subgroups**

3.3.1. *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.

3.3.2. *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. This is easy manipulation — see Problem 3.14. □

There is another, very useful, characterization of normal subgroups in §5.2.1 later.

3.3.3. *Lemma.* Let $\phi : G \to H$ be a group homomorphism. Then $\ker\phi \trianglelefteq G$.

Proof. See Problem 3.15. □

3.3.4. *Theorem.*

1. If G is abelian, then every subgroup of G is normal.
2. $G \trianglelefteq G$ and $\{e\} \trianglelefteq G$.
3. Let $H \leq G$ with $|G| = 2\,|H|$. Then H is normal in G.

Proof. Parts 1 and 2 are immediate from the definition. For part 3, we know that there are precisely $\frac{|G|}{|H|} = 2$ distinct left cosets of H (by §2.9.8) so one must be H, the other $G \backslash H = \{g \in G \mid g \notin H\}$. Similarly, by the right coset version of §2.9.8, there are precisely $\frac{|G|}{|H|} = 2$ distinct right cosets of 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 §3.3.2, H is normal in G. □

3.4. **Quotient groups**

3.4.1. *Lemma.* Let $N \trianglelefteq G$ and suppose $n \in N$ and $g \in G$. Then there exists $n' \in N$ such that $gn = n'g$. (Similarly there exists $n'' \in N$ such that $ng = gn''$.)

Proof. 1. Since $g \in G$ and $n \in N$, by the definition of normal subgroup we have $gng^{-1} \in N$, say $gng^{-1} = n'$. Then $gn = n'g$.
2. Since $g^{-1} \in G$ and $n \in N$, by the definition of normal subgroup we have $g^{-1}n(g^{-1})^{-1} = g^{-1}ng \in N$, say $g^{-1}ng = n''$. Then $ng = gn''$. □

Up until now, when H is a subgroup of G we have studied G/H, the set of left cosets of H in G. I emphasize that this is only a *set* in general. However, when H is a normal subgroup, we can endow the set G/H with the structure of a group:

3.4.2. *Theorem.* Let $N \trianglelefteq G$. Then

$$gN * hN := ghN$$

defines a group structure on the set G/N. The identity is eN ($= N$ by §2.9.6 part 1), and the inverse of gN is $g^{-1}N$.

Proof. Since it is possible that $g_1N = g_2N$ even when $g_1 \neq g_2$, we must prove that the above operation is well-defined. To see this, suppose $g_1N = g_2N$ and $h_1N = h_2N$. We need to show that $g_1N * h_1N = g_2N * h_2N$. Now $g_1 = g_2n$ for some $n \in N$ and $h_1 = h_2m$ for some $m \in N$, thus by §3.4.1

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

as required.
Thus the above operation is well-defined and clearly satisfies the closure axiom. The fact that the operation is associative follows easily from the corresponding fact for G. The fact that eN serves as an identity is just

$$gN * eN := (ge)N = gN = (eg)N := eN * gN.$$

for all $gN \in G/N$. The fact that gN has an inverse $g^{-1}N$ can be checked similarly. □

3.4.3. *Definition.* When $N \trianglelefteq G$, we call the set G/N equipped with the group operation $gN * hN := ghN$ the *quotient group of G by N.*

Again I emphasize that N is required to be normal for the set G/N to be a group. Thus 'quotient group' only makes sense for normal subgroups.

3.4.4. *Philosophy.* Why bother?

1. Usually we want to understand a finite group G. Say we can find a normal subgroup $N \neq \{e\}$. Then both N and G/N are groups, and both $|N|$ and $|G/N|$ are strictly smaller than $|G|$. We hope to understand both these smaller groups, then try and piece together this information to understand G.
2. Passing to a factor is useful for induction arguments.

There are lots of other reasons too, and I will discuss some in the lecture.

3.4.5. *Examples.*

1. (This comment will only make sense after Semester 2). Quotient constructions are very common in mathematics, and you will see an example next semester. Let V be a vector space with subspace W. Thinking of V as an abelian group under addition, and W as a (necessarily normal since V is abelian) subgroup of V, then the quotient group V/W is the same thing as the quotient vector space that will be defined next semester. (Vector spaces also have scalar multiplication that we are neglecting in this.) To see this, when $W \subseteq V$ is a subspace, next semester you will define a relation $x \sim y \iff x - y \in W$, and then define V/W to be the set of equivalence classes. Note that since W

is a group under addition, really this relation is $x \sim y \iff x * y^{-1} \in W$, so $x \sim y \iff x * W = y * W$. Thus the set of equivalence classes is the set of left cosets of W in V.

2. Fix $n \in \mathbb{N}$ and define $n\mathbb{Z} := \{kn \,|\, k \in \mathbb{Z}\}$. Then $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, which is normal since $\mathbb{Z}$ is abelian. We will see in §3.6.4 that the quotient group $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

3.5. **Defining homomorphisms out of the quotient**

Suppose that $N \trianglelefteq G$, and H is some other group. How to define a group homomorphism $G/N \to H$? For example, how to define a homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$? The main problem is that we must ensure that the map is well-defined, i.e. if $g_1 N = g_2 N$ then we have to ensure that $g_1 N$ and $g_2 N$ are sent to the same object. To save you having to check this every time, the following is useful:

3.5.1. *Theorem.* Suppose $N \trianglelefteq G$ and $\phi : G \to H$ is a group homomorphism. If $N \subseteq \operatorname{Ker}\phi$, then ϕ induces a well-defined group homomorphism $\hat{\phi} : G/N \to H$ defined by $gN \mapsto \phi(g)$.

Proof. We show that $\hat{\phi}$ is well-defined, the rest is easy to check. If $g_1 N = g_2 N$, then $g_1^{-1} g_2 \in N \subseteq \operatorname{Ker}\phi$ and so $\phi(g_1^{-1} g_2) = e_H$. But ϕ is a group homomorphism so

$$e_H = \phi(g_1^{-1} g_2) = \phi(g_1^{-1})\phi(g_2) = \phi(g_1)^{-1}\phi(g_2),$$

which implies that $\phi(g_1) = \phi(g_2)$. Thus $\hat{\phi}(g_1 N) := \phi(g_1) = \phi(g_2) := \hat{\phi}(g_2 N)$ and so $\hat{\phi}$ is well-defined. □

3.5.2. *Example.* Define $\phi : \mathbb{Z} \to \mathbb{Z}_n$ by taking the remainder mod n. This is a group homomorphism. Clearly $n\mathbb{Z}$ gets sent to zero, so $n\mathbb{Z} \subseteq \operatorname{Ker}\phi$. Thus by §3.5.1 there is a well-defined group homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$.

3.6. **The first isomorphism theorem**

3.6.1. *Lemma.* Let $N \trianglelefteq G$. Then there is a canonical surjective homomorphism of groups $p : G \to G/N$ defined by $p : g \mapsto gN$. The kernel of p is N.

Proof. This is an easy consequence of the definitions. Make sure that you can prove this. □

Now given any group homomorphism $\phi : G \to H$, we know by §3.3.3 that $\operatorname{Ker}\phi \trianglelefteq G$, and so $G/\operatorname{Ker}\phi$ is a group. This has another, easier description:

3.6.2. *Theorem.* **(First isomorphism theorem for groups)** Let $\phi : G \to H$ be a homomorphism of groups. Then $G/\operatorname{Ker}\phi \cong \operatorname{Im}\phi$ in such a way that the following diagram commutes:

$$\begin{tikzcd}
G \arrow[r, "p"] \arrow[dr, "\phi"'] & G/\operatorname{Ker}\phi \arrow[d, dotted, "\hat{\phi}"] \\
 & \operatorname{Im}\phi
\end{tikzcd}$$

Proof. Denote $K := \operatorname{Ker}\phi$. Since $K \trianglelefteq G$, we may apply §3.5.1 to obtain a well-defined group homomorphism $\hat{\phi} : G/K \to \operatorname{Im}\phi$ defined by $\hat{\phi}(gK) := \phi(g)$. It is surjective by definition of $\operatorname{Im}\phi$. For injectivity, if $\hat{\phi}(gK) = e_H$ then $\phi(g) = e_H$ and so $g \in K$. This implies that $gK = K = e_{G/K}$, and so $\operatorname{Ker}\hat{\phi} = \{e_{G/K}\}$. By §3.1.5 part 3, $\hat{\phi}$ is injective. □

3.6.3. *Slogan.* The most important aspect of the above is that if $\phi : G \to H$ is a group homomorphism, then *"the image of ϕ is isomorphic to the quotient $G/\ker\phi$"*. More informally, the information that you are left with after applying ϕ (i.e. the image $\operatorname{Im}\phi$) is the same (=isomorphic) to the information that you started with (i.e. G) modulo the information that is lost (i.e. $\operatorname{Ker}\phi$).

3.6.4. *Examples.*

1. Fix $n \in \mathbb{N}$ and consider the surjective group homomorphism $R : \mathbb{Z} \to \mathbb{Z}_n$ given by taking the remainder mod n. The kernel is clearly $n\mathbb{Z}$ and so the first isomorphism theorem shows $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\operatorname{Ker}R \cong \operatorname{Im}R = \mathbb{Z}_n$, i.e. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.
2. Consider the surjective homomorphism $\exp : \mathbb{C} \to \mathbb{C}^*$ (the former under addition and the latter under multiplication). The kernel is $N = \{2k\pi i \mid k \in \mathbb{Z}\}$. So $\mathbb{C}^*$ is isomorphic to $\mathbb{C}/N$.

4. Actions of Groups

4.1. Definition of a group action

4.1.1. *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 $x \in X$.

4.1.2. *Examples.*

1. Roughly speaking, if G is the symmetry group of an object, then G acts on that object. Like §1.3 this is a little vague, but is made precise in the following examples:
   (a) Let G be the symmetry group of a graph, and let V be the set of vertices of the graph. Then G acts on V by $g \cdot x := g(x)$. The first axiom follows from properties of functions, whereas the second axiom follows since the identity e is the identity map.
   (b) The symmetric group S_n acts on the set $\{1, 2, \dots, n\}$. This is a special case of (a).
   (c) The group D_n acts on the set $\{1, 2, \dots, n\}$, where we think of the numbers as labeling the vertices of the n-gon. This is a special case of (a).
   (d) 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 $f(v_1)$ and $f(v_2)$.
2. 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).
3. 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*.
4. 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

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

(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

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

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

4.2. **Faithful actions**

4.2.1. *Theorem.* Suppose G acts on X. Define

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

(So N consists of all the elements of G that do not move anything in X. We say that such g "act trivially".) Then N is a normal subgroup of G.

Proof. 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

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

for all $x \in X$ and so $n_1 n_2 \in N$. 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. For normality, let $n \in N$ and $g \in G$. Then

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

for all $x \in X$ and so $gng^{-1} \in N$. Hence $N \trianglelefteq G$. □

4.2.2. *Definition.* In the notation above, 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".

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

If X is a set, we denote $\text{bij}(X)$ to be the group of bijections $X \to X$. Note that if X is finite, then $\text{bij}(X)$ is the symmetric group $S_{|X|}$

4.3.1. *Theorem.* Let G be a group, and let X be a set. Then

1. An action of G on X is the same thing as a group homomorphism $\phi : G \to \text{bij}(X)$.
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 $\operatorname{im} \phi \leq \text{bij}(X)$.

Proof. 1. Suppose that $\cdot$ defines an action, then define $\phi : G \to \text{bij}(X)$ by $g \mapsto L_g$, where $L_g : X \to X$ takes $x \mapsto g \cdot x$. You can check that L_g is a bijection, and that ϕ is a group homomorphism. Conversely, given a group homomorphism $\phi : G \to \text{bij}(X)$, define $g \cdot x := \phi(g)(x)$. You can check that this gives a group operation, and that these are inverse operations.

2. is an easy exercise, using the fact that a homomorphism $\theta : G \to H$ is injective if and only if $\operatorname{Ker}\theta = \{e_G\}$ (see Problem 3.1).
3. By part 2, there is an injective group homomorphism $\phi : G \to \operatorname{bij}(X)$, so the result follows easily (see §3.1.5 part 4). □

4.3.2. *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 §4.3.1 (part 3), G is isomorphic to a subgroup of $S_{|G|}$. □

4.3.3. *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 4.12 later) is thus a subgroup of S_{60}. 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 §4.3.1 part 3, G is also a subgroup of $\operatorname{bij}(X) = S_{|X|} = S_{12}$.
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
$$C_3 = \langle g \rangle \cong \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rangle \leq S_3.$$

4.4. Non-faithful actions induce faithful ones

4.4.1. *Theorem.* Suppose G acts on a set X. Define
$$N = \{g \in G \,|\, g \cdot x = x \quad \text{for all } x \in X\} \trianglelefteq G$$
as before. If the action of G on X is not faithful, then the quotient group G/N acts on X. This action is faithful.

Proof. Consider the group homomorphism $G \to \operatorname{bij}(X)$ that describes the group action (as in §4.3.1 part 1). The kernel is N, so by the first isomorphism theorem we have
$$G/N \overset{\cong}{\to} \operatorname{Im} \leq \operatorname{bij}(X).$$
In particular we have an injective group homomorphism $G/N \to \operatorname{bij}(X)$, hence G/N acts on X (by §4.3.1 part 1), and furthermore (by §4.3.1 part 2) the action is faithful. □

4.4.2. *Examples.*

1. As in §4.1.2 part 2, consider D_n acting on $X := \{T, B\}$ (standing for "top" and "bottom" of the n-gon) by swapping T and B if the symmetry turns the n-gon over. Then the subgroup of rotations $\{e, g, \dots, g^{n-1}\} = C_n$ is precisely the subgroup that acts trivially, hence the quotient D_n/C_n acts faithfully on X by §4.4.1. Note that $D_n/C_n \cong C_2$ by Problem 3.18.
2. (harder) Consider the set X of all groupings of 4 objects into two pairs:

$$X := \{[1, 2; 3, 4], [1, 3; 2, 4], [1, 4; 2, 3]\}.$$

Then S_4 acts on X in an obvious way. The subgroup that acts trivially is $K = C_2 \times C_2$. Thus we see that S_4/K is isomorphic to S_3.

4.5. **Orbits and Stabilizers**

4.5.1. *Definition.* Let $x \in X$ and suppose that G acts on X. The *stabilizer* of x is defined to be

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

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

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

Proof. See Problem 4.5. □

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

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

4.5.4. *Examples.*

1. 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 §4.1.2, part 4.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

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

2. 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.
3. See Problems 4.5 – 4.10 for more examples of orbits and stabilizers.

4.5.5. *Theorem.* 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 $x \sim y$. 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 exist $g, h \in G$ 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 $x \sim z$.

The fact that the equivalence classes are the orbits follows straight from the definition. □

4.5.6. *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.

4.5.7. *Examples.*

1. For any given graph, as in §4.1.2 part 1(a) the group of symmetries acts on the set of vertices. This action may or may not be transitive (see Problem 4.3).
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 $v_1 = g \cdot v_2$. Also, the action is faithful since if an element leaves all the vertices fixed, it must be the identity.

Recall 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.

4.5.8. *Proposition.* Let G act on X, and let $x \in X$. Then the map

$$\phi : G/\operatorname{Stab}_G(x) \to \operatorname{Orb}_G(x) \quad \text{which sends} \quad g \operatorname{Stab}_G(x) \mapsto g \cdot x$$

is well-defined and is a bijection of *s*ets.

Proof. Denote $H := \operatorname{Stab}_G(x)$. If $g_1H = g_2H$ then $g_2 = g_1h$ for some $h \in H$. This implies that

$$g_2 \cdot x = (g_1h) \cdot x = g_1 \cdot (h \cdot x) = g_1 \cdot x,$$

hence $\phi(g_1H) = \phi(g_2H)$ and so ϕ is well-defined. Clearly the image of ϕ is the whole of the orbit of x, and so ϕ is surjective. To see that ϕ is injective, suppose that $\phi(g_1H) = \phi(g_2H)$. Then $g_1 \cdot x = g_2 \cdot x$, so acting with g_1^{-1} on both sides we get

$$(g_1^{-1}g_2) \cdot x = (g_1^{-1}g_1) \cdot x = e \cdot x = x.$$

Hence $g_1^{-1}g_2 \in H$ and so $g_1H = g_2H$ (by §2.9.6 part 2). Thus ϕ is injective. □

4.5.9. *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 §4.5.8 $|\mathrm{Orb}_G(x)| = |G/\,\mathrm{Stab}_G(x)|$. By §2.9.8 this is equal to $\frac{|G|}{|\mathrm{Stab}_G(x)|}$. □

4.5.10. *Examples.* The orbit–stabilizer theorem is useful both theoretically (see §5, in particular §5.5.2) and computationally (see below, and the problem sheets, for nice applications), so it is very important.

1. (Order of the dihedral group) The dihedral group acts transitively on the set V of vertices of the n-gon (§4.5.7). Pick a vertex $v \in V$, and suppose $g \in D_n$ fixes v. It is very easy to show (argue as in §1.4.4) that the only elements of D_n which fix v are the identity and the reflection in the line through v. Hence $|\mathrm{Stab}_{D_n}(v)| = 2$. Since the action is transitive, $V = \mathrm{Orb}(v)$ and so by orbit–stabilizer $|D_n| = |\mathrm{Stab}_{D_n}(v)| \times |V| = 2 \times n = 2n$. This gives a slightly less painful proof of Problem 1.3.
2. (Order of the groups of rotational symmetries of Platonic solids) Let G be the rotational symmetry group of the cube. Consider G acting on the set E of 12 edges. This action is transitive (convince yourself that you can take any edge to any other edge just by rotating). Pick an edge $e \in E$, then the stabilizer is just the identity together with the rotation about the centre of that edge. Thus $|G| = |\mathrm{Stab}_G(e)| \times |E| = 2 \times 12 = 24$. Hence there are precisely 24 rotational symmetries of the cube. This implies that if we can write down 24 distinct symmetries, we have them all (see §4.6.2 part 2). A similar argument applies to all Platonic solids — see Problem 4.12.

4.6. **Pólya counting**

A beautiful application of group theory.

4.6.1. *Theorem.* 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

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

Proof. Define

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

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 orit–stabilizer

$|\mathrm{Stab}(x)| = \frac{|G|}{|\mathrm{Orb}(x)|}$, and so on comparing expressions for $|Z|$ we see that

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

Hence $\frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}(g)| = \sum_{x\in X} \frac{1}{|\mathrm{Orb}(x)|}$ = the number of G-orbits in X. □

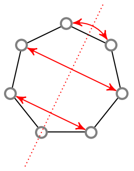
4.6.2. *Example.*

1. How many essentially different ways are there of colouring the vertices of a regular heptagon 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 §4.6.1 we must analyse the fixed points.

   - The identity fixes every coloured heptagon in X, so $|\mathrm{Fix}(e)| = 2187$.
   - Consider any non-trivial rotation (there are 6 of them). Clearly the only way a colored heptagon 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 heptagon 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 the number of orbits is equal to

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

2. How many ways are there of colouring the faces of a cube with 3 colours? Two colourings are regarded as the same if they differ by an element of the rotational symmetry group (which we know by §4.5.10 consists of 24 elements). These are difficult to TeX, so see for example

   http://www.youtube.com/watch?v=gBg4-IJ19Gg

   There are 8 non-trivial rotations (of order 3) about vertices, 6 half-turns (of order 2) about the centres of edges, and 9 non-trivial rotations about the centres of faces (which come in two different sorts, quarter-turns and half-turns), and then the identity. Since we have written down 24 distinct symmetries, and we know by §4.5.10 there are precisely 24, we have written down them all.

The fixed point analysis is

Type of element	Number	Fixed points per element
e	1	$3^6 = 729$
$\pm(1/3)$-turn about vertex	8	$3^2 = 9$
$(1/2)$-turn about centre of edge	6	$3^3 = 27$
$\pm(1/4)$-turn about centre of face	6	$3^3 = 27$
$(1/2)$-turn about centre of face	3	$3^4 = 81$

Hence the number of colourings, i.e. the number of orbits, is equal to

$$\frac{1}{24}(729 + (8 \times 9) + (6 \times 27) + (6 \times 27) + (3 \times 81)) = 57.$$

5. Properties of Groups from Counting

Here we basically let G act on itself, then apply the results of the last section.

5.1. Conjugate elements

5.1.1. *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

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

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

5.1.2. *Examples of conjugacy classes.*

1. See Problem 5.8 for the conjugacy classes in D_4.
2. See §6 for conjugacy in the symmetric group S_n (and also conjugacy in another group, A_n).

5.1.3. *Definition.*

1. We say that g, g' are *conjugate* if there exists $h \in G$ such that $g' = hgh^{-1}$. Thus two elements of G are conjugate if and only if they are in the same orbit under the conjugate action defined in §5.1.1.
2. 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.

5.1.4. *Corollaries.*

1. The centralizer $C(g)$ of $g \in G$ 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

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

Proof. If G acts on X, then $\mathrm{Stab}(x)$ is always a subgroup of G (by §4.5.2), so 1 follows as a special case. Since $C(G) = \bigcap_{g\in G} C(g)$, the second result follows because an intersection of subgroups is always a subgroup. The last result is just the orbit-stabilizer theorem. □

5.1.5. *Properties.*

1. The group G is partitioned into conjugacy classes.
2. $\{e\}$ is always a conjugacy class of G
3. $\{g\}$ is a conjugacy class if and only if $g \in C(G)$. (So $C(G)$ is the union of all the one-element conjugacy classes.)

5.1.6. *Examples of centres of groups.*

1. G is abelian if and only if $C(G) = G$.
2. If $n > 2$, then $C(S_n) = \{e\}$. It is not too hard to see that only the identity permutation commutes with every other permutation.
3. In $\mathrm{GL}(n,k)$ the centre is $\{\lambda\mathbb{I} \mid \lambda \in k\}$. See Problem 5.6.

5.2. Normal subgroups and conjugacy classes

5.2.1. *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 $gng^{-1} \in N$ 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. □

5.2.2. *Corollary.* If G is a group, then the centre $C(G)$ is a normal subgroup.

Proof. The centre is the union of all one-element conjugacy classes (by §5.1.5), so the result follows from §5.2.1. □

5.3. The class equation

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

1. Let $g \in C_k$. Then $c_k = \frac{|G|}{|C(g)|}$. In particular, c_k divides the order of the group.
2. We have
$$|G| = c_1 + c_2 + \dots + c_n,$$
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 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. □

5.3.2. *Examples.*

1. See Problems 5.9 – 5.10 for examples of the class equation.
2. See Problem 6.13 for the use of the class equation in a problem which doesn't seem to directly involve it.

5.4. **Two useful theorems**

The class equation has theoretical consequences:

5.4.1. *Theorem.* If $|G| = p^k$ where p is prime and $k \in \mathbb{N}$, then $|C(G)| \geq p$.

Proof. Consider the class equation

$$|G| = c_1 + \dots + c_n.$$

Every conjugacy class has size 1 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 1. The centre of G is the union of all the 1-element conjugacy classes (by §5.1.5) and so the result follows. □

5.4.2. *Theorem.* Every group G of order p^2 (where p is prime) is abelian.

Proof. By the previous result 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. □

5.5. **Sylow's 1st Theorem**

Just by counting, we obtain strong structural results about the existence of subgroups.

5.5.1. *Definition.* Let $p \in \mathbb{N}$ be a prime. A finite group G is called a p-group if $|G| = p^t$ for some $t \in \mathbb{N}$.

5.5.2. *Theorem.* **(1st Sylow Theorem)** Let G be a finite group and let p be a prime factor of $|G|$. Suppose that $k \in \mathbb{N}$ is largest such that p^k divides $|G|$. Then G contains a subgroup H such that $|H| = p^k$.

Proof. Write $|G| = p^k m$, where $\gcd(p, m) = 1$. Consider the set $\mathcal{S}$ of all subsets of U of G with $|U| = p^k$. The number of such subsets is

$$|\mathcal{S}| = \binom{p^k m}{p^k} = \frac{p^k m}{p^k} \times \frac{p^k m - 1}{p^k - 1} \times \dots \times \frac{p^k m - p^k + 1}{1}.$$

If in each term $\frac{p^k m - j}{p^k - j}$ we cancel all common divisors of the numerator and denominator, p does not remain a divisor of the numerator. To see this (it is clear for $j = 0$), let $j > 0$ then we may certainly write j as $j = p^l s$, where $l, s \in \mathbb{N} \cup \{0\}$ and $\gcd(p, s) = 1$. Then $l < m$, so

$$\frac{p^k m - j}{p^k - j} = \frac{p^{k-l} m - s}{p^{k-l} - s}.$$

Certainly p does not divide $p^{k-l}m - s$, and hence since p is prime, it follows that p does not divide the product of the numerators. Therefore $p \nmid |\mathcal{S}|$.

For $U \in \mathcal{S}$ and $g \in G$, gU is a subset of G with $|Ug| = |U|$, thus $gU \in \mathcal{S}$. Clearly, it is seen that G acts on the set $\mathcal{S}$ by left multiplication. Under this action $\mathcal{S}$ is partitioned into orbits, and it follows (since $p \nmid |\mathcal{S}|$) that there exists an orbit $\mathcal{A}$ such that $p \nmid |\mathcal{A}|$. Pick an element V of $\mathcal{S}$ which belongs to the orbit $\mathcal{A}$, and set $H := \mathrm{Stab}_G(V) \leq G$. By orbit–stabilizer,

$$|\mathcal{A}| = \frac{|G|}{|H|}.$$

Thus $p^k m = |G| = \frac{|G|}{|H|}|H| = |\mathcal{A}|\,|H|$. But $p \nmid |\mathcal{A}|$, so necessarily p^k divides $|H|$.

We now show $|H| = p^k$, as this then completes the proof. Since p^k divides $|H|$ by above, it suffices to show that $|H| \leq p^k$. To do this, since $|V| = p^k$, let $V = \{x_1, x_2, ..., x_{p^k}\}$ denote the elements of V. Then for any $h \in H = \mathrm{Stab}_G(V)$, $hV = V$, that is

$$\{hx_1, hx_2, ..., hx_{p^k}\} = \{x_1, x_2, ..., x_{p^k}\}.$$

Hence $hx_1 = x_i$ for some i with $1 \leq i \leq p^k$, and so $h = x_i x_1^{-1}$. This shows that

$$H \subseteq \{e, x_2x_1^{-1}, x_3x_1^{-1}, \dots, x_{p^k}x_1^{-1}\},$$

hence $|H| \leq p^k$, as required. □

5.5.3. *Corollary.* **(Cauchy's Therem)** Let G be a finite group and let p be a prime factor of $|G|$. Then G contains an element of order p (and hence a cyclic subgroup of order p).

Proof. By §5.5.2 there exists a subgroup H of G with $|H| = p^k$. Pick $h \in H$ with $h \neq e$. Then $o(h)$ divides p^k, say $o(h) = p^s$, with $s \geq 1$. If $s = 1$ then $o(h) = p$ and so we are done. If $s > 1$, then $h^{p^{s-1}}$ has order p (check this!). □

6. **Symmetric Groups**

By §4.3 we know that every finite group lives inside a symmetric group.

6.1. **Basics**

Recall that the symmetric group S_n is the group of all permutations of n objects (usually thought of as the numbers $\{1, 2, \dots, n\}$). It has order $n!$. Recall also the notation that $\sigma \in S_n$ is specified by the 2-row array

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

6.1.1. *Composition: method 1.* For example, in S_6 consider

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$$

Recall that for permutations, as for other maps, our convention is $\sigma\tau$ means "do τ *then* do σ". Thus under the first map 1 gets sent to 2, which under the second map gets sent to 1. Hence overall $1 \mapsto 1$. Similarly 2 gets sent to 4, which then gets sent to 3, so overall $2 \mapsto 3$. Continuing in this way, by exhausting all possibilities we see that

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

For many of our purposes, the above matrix notation for elements of S_n is not very good, and so we introduce cycle notation:

6.1.2. *Definition.* Let $n \in \mathbb{N}$, let $1 \le r \le n$ and let $\{a_1, a_2, \dots, a_r\}$ be r distinct numbers between 1 and n. The *cycle* $(a_1\, a_2\, \dots\, a_r)$ 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 $(a_1\, a_2\, \dots\, a_r)$ is r.

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

6.1.3. *Example.* Thus (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

$$\begin{tikzcd}[column sep=small] (& 2 \arrow[r, bend right] & 1 \arrow[r, bend right] & 4 \arrow[ll, bend right] &) \end{tikzcd}$$

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

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

in the 2-row array notation.

6.1.4. *Composition: method 2.* In S_6, consider the cycles (1623) and (14235). Their composition

$$(1623)(14235)$$

(recall the convention that we do the right one first, then the left) sends 1 to 4 (to 4), 2 to 3 to 1, 3 to 5 (to 5), 4 to 2 to 3, 5 to 1 to 6, (6 to) 6 to 2. Hence overall this is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 3 & 6 & 2 \end{pmatrix}.$$

6.2. **Disjoint cycles**

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

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

6.2.2. *Note.* Composition of disjoint cycles is commutative (prove this — see Problem 6.3) and so e.g. (1534)(27) = (27)(1534).

6.2.3. *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 any introductory textbook on Group Theory). 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

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

□

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

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

etc, in any order.

6.2.5. *Example.* Continuing the example in §6.1.4,

$$(1623)(14235) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 3 & 6 & 2 \end{pmatrix} = (143562).$$

With a bit of practice, you can go from the left hand side to the right hand side in one step.

6.3. Generators of the symmetric group

6.3.1. *Definition.* A cycle of length two is called a *transposition*. For example (23) and (14) are transpositions.

6.3.2. *Theorem.* Every permutation can be written as a composition of transpositions. Thus, S_n is generated by transpositions.

Proof. Let T be the set of transpositions. Always $\langle T\rangle \leq S_n$. Conversely, let $\sigma \in S_n$, then by §6.2.3 we can write σ as the product of disjoint cycles. Thus since every cycle

$$(x_1x_2 \dots x_k) = (x_1x_2)(x_2x_3)\dots(x_{k-1}x_k),$$

σ is a product of transpositions, and hence $\sigma \in \langle T\rangle$. This shows that $S_n \subseteq \langle T\rangle$ and so $\langle T\rangle = S_n$. □

6.3.3. *Application.* Consider the group G of symmetries of the cube, acting on the set X of diagonals of the cube. Note that $|X| = 4$. Define the group homomorphism $\phi : G \to S_4 = S_{|X|}$ as in §4.3.1. Now no non-identity element of the cube fixes all the diagonals (we know all 24 rotational symmetries, so just check each), hence ϕ is injective. Also, one can find a "half-turn about centres of edges" that acts as a transposition on two given diagonals and fixes the other two. Thus inside $\operatorname{Im}\phi$ are all transpositions. Since $\operatorname{Im}\phi$ is a subgroup, it is closed under multiplication, and so by §6.3.2 $\operatorname{Im}\phi = S_4$. Hence

- $G \cong S_4$ (via ϕ).
- The six "half-turns about centres of edges" generate the rotational symmetries of a cube.

6.4. Cycle type and their number

6.4.1. *Definition.* Given $\sigma \in S_n$, write σ as a product of disjoint cycles, as in §6.2.3. 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 6.5.

6.4.2. *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.

6.4.3. *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. (sketch) A permutation of the given cycle type is produced by filling $\{1, 2, \dots, n\}$ into the blanks in the following pattern:

$$\underbrace{(\bullet)\dots(\bullet)}_{m_1}\underbrace{(\bullet\bullet)\dots(\bullet\bullet)}_{m_2}\underbrace{(\bullet\bullet\bullet)\dots(\bullet\bullet\bullet)}_{m_3}\dots$$

There are $n!$ ways of doing this, but we must account for the fact that some of these ways give the same element of S_n.

- Since $(a)(b) = (b)(a)$, the one-cycles can be permuted and this gives the same element. Similarly for the 2-cycles, etc. There are $m_1!$ permutations of the 1-cycles, $m_2!$ permutations of the 2-cycles, etc, so we must divide by $m_1! \dots m_n!$
- Each 2-cycle has two different ways of being written (since $(ab) = (ba)$). Similarly each 3-cycle has three different ways of being written (since $(abc) = (bca) = (cab)$), etc, and so we must also divide by $1^{m_1} 2^{m_2} \dots n^{m_n}$.

□

6.4.4. *Examples.*

1. How many elements of type $1, 1, 3, 4$ 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 $\frac{9!}{2.1.1.1^2.3^1.4^1} = 15120$.
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.

6.5. Conjugacy in S_n is determined by cycle type

6.5.1. *Lemma.* Let $\sigma \in S_n$, and write σ as a product of disjoint cycles, say $\sigma = (a_1 \dots a_r)(b_1 \dots b_s) \dots$. Then for all $\tau \in S_n$,

$$\tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_r))(\tau(b_1) \dots \tau(b_s)) \dots$$

which is a product of disjoint cycles.

Proof. We just have to check that the right hand side acts on every element in $\{1, \dots, n\}$ in the same way as $\tau\sigma\tau^{-1}$. 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. □

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

Proof. ($\Rightarrow$) is §6.5.1.
($\Leftarrow$) 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 §6.5.1 shows that $\tau\sigma\tau^{-1}$ and γ are the same element. □

6.5.3. *Examples.*

1. How many elements are conjugate to $(123)(4567)(8)(9)$ in S_9? By the theorem, this is equal to the number of elements of type $1, 1, 3, 4$. By §6.4.4, this is equal to 15120.
2. By the above theorem and §6.4.4 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 6.9.

6.6. The alternating groups

6.6.1. *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*.

6.6.2. *Theorem.* Let A_n denote the set of all even permutations in S_n. Then A_n is a normal 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 §4.5.2). Its order follows immediately from the orbit-stabilizer theorem. Since $|A_n| = \frac{|S_n|}{2}$ it follows immediately that $A_n \trianglelefteq S_n$ (by §3.3.4). □

6.6.3. *Remark.* Since $A_n \trianglelefteq S_n$ we can form the factor group S_n/A_n. We know from the above that this has order two, hence it must be isomorphic to C_2.

6.6.4. *Theorem.*

1. The product of two even permutations is even. The product of two odd permutations is even. The product of an odd and an even permutation is odd.
2. Transpositions are odd.
3. A permutation is even if and only if it can be written as a product of an even number of transpositions.
4. A cycle of length k is even if k is odd, and the cycle is odd if k is even.

Proof. 1. If σ and τ are both odd, then

$$(\sigma\tau) \cdot P = \sigma \cdot (\tau \cdot P) = \sigma(-P) = P$$

and so $\sigma\tau$ is even. The rest are similar.

2. Suppose σ is the transposition swapping 1 and 2. Then in the factorization of P, the factor $(x_1 - x_2)$ changes sign under the action of σ. No other factors involving x_1 change sign. The only factors involving x_2 that remain are $(x_2 - x_j)$ for $j = 3, \dots, n$, and none of these change sign under σ. Hence $\sigma \cdot P = -P$ and so σ is odd. The general case (i.e. σ is an arbitrary transposition) is similar.

3. $(\Leftarrow)$ is obvious from part 1. For $(\Rightarrow)$, pick $\sigma \in A_n$ then by §6.3.2 σ can be written as a product of transpositions. By part 1, necessarily there must be an even number.

4. Follows from the formula

$$(x_1 x_2 \dots x_k) = (x_1 x_2)(x_2 x_3) \dots (x_{k-1} x_k)$$

together with parts 1 and 2. □

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

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

6.7. **Application**

6.7.1. *Theorem.* Let G be the group of rotational symmetries of the tetrahedron. Then $G \cong A_4$.

Proof. G acts on the set X of 4 vertices, thus as in §4.3.1 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 $G \cong \operatorname{Im}\phi$. 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 $G \cong A_4$. □

7. Groups of Small Size

7.1. Finite abelian groups

As before, let C_n denote the cyclic group of order n.

7.1.1. *Theorem.* The product $C_m \times C_n$ is isomorphic to C_{mn} if and only if m, n are relatively prime (i.e. $\gcd(m, n) = 1$).

Proof. Note that $C_m \times C_n$ has mn elements. So as not to confuse notation, let $C_m = \langle g \rangle$ and $C_n = \langle h \rangle$.
($\Leftarrow$) Suppose m, n are relatively prime and let $x = (g, h)$. Then $x^k = (g^k, h^k)$, which equals the identity if and only if k is a multiple of both m and n. But the least such k is mn and so x has order mn. Hence $C_m \times C_n$ is cyclic, and therefore (by §3.1.4 part 2) isomorphic to C_{mn}.
($\Rightarrow$) (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 $(x, y) \in C_m \times C_n$, then $(x, y)^k = (x^k, y^k) = (e, e) = e_{C_m \times C_n}$. Hence $C_m \times C_n$ has no element of order mn, and so therefore it cannot be cyclic. □

7.1.2. *Theorem.* Let $G = C_{j_1} \times \ldots \times C_{j_n}$ be a product of cyclic groups. Then G is isomorphic to a product $G = C_{k_1} \times \ldots \times C_{k_m}$ where k_i divides k_{i+1} for all $i = 1, \ldots, m-1$. We will say that products of cyclic groups of this type are in *standard form*.

Proof. You should try and prove this, based on the procedure in the example below. □

7.1.3. *Examples.*

1. Consider $C_{12} \times C_{18}$. We begin by writing 12 and 18 as products of powers of primes, i.e. $12 = 2^2.3$ and $18 = 2.3^2$. Now

$$\begin{aligned} C_{12} \times C_{18} &\cong (C_{2^2} \times C_3) \times (C_2 \times C_{3^2}) \\ &\cong (C_2 \times C_3) \times (C_{2^2} \times C_{3^2}) \\ &\cong C_6 \times C_{36}, \end{aligned}$$

   where the first and third isomorphisms follow from §7.1.1. The principle behind the rearrangement in the second line is that the right-hand term contains the highest power of every prime that occurs, whilst the left-hand term contains the second-highest (if that exists).

2. Consider instead $C_{24} \times C_{36} \times C_{30}$. Then

$$\begin{aligned} C_{24} \times C_{36} \times C_{30} &\cong (C_{2^3} \times C_3) \times (C_{2^2} \times C_{3^2}) \times (C_2 \times C_3 \times C_5) \\ &\cong (C_2 \times C_3) \times (C_{2^2} \times C_3) \times (C_{2^3} \times C_{3^2} \times C_5) \\ &\cong C_6 \times C_{12} \times C_{360}. \end{aligned}$$

Again, the rightmost term has the highest power of each prime that appears, the middle contains the second-highest and the leftmost the third-highest power.

7.1.4. *Two facts that we don't have time to prove.*

1. If two products of cyclic groups have different standard forms then they are not isomorphic.
2. Every finite abelian group is isomorphic to a product of cyclic groups.

If we had time to prove these facts, then we would have completely classified finite abelian groups. In what follows we will assume §7.1.4 and try to classify all groups of small order, up to isomorphism. Thus when we say that "there is only one group of order 5" we really mean that all groups of order 5 are isomorphic.

7.2. **Nonabelian groups**

We already know all finite abelian groups from §7.1.4, so we search for possible nonabelian groups.

7.2.1. *Theorem.* If G is a group with $|G| \leq 12$, then if G is not abelian, necessarily $|G|$ must be either 6, 8, 10 or 12.

Proof. We already know that every group of order p or p^2 (where p is a prime) is abelian. See Problem 5.11 if this is unclear. This means that the only possibilities are 6, 8, 10 or 12. □

We already know examples of nonabelian groups of orders 6, 8, 10 and 12 — namely D_3, D_4, D_5 and D_6. We search for more:

7.2.2. *Theorem.* Suppose that G is a nonabelian group with $|G| = 2p$, where p is an odd prime. Then $G \cong D_p$. In particular, the only nonabelian group of order 6 is D_3 (so $D_3 \cong S_3$), and the only nonabelian group of order 10 is D_5.

Proof. By Cauchy's Theorem (§5.5.3), G contains an element x of order p, and hence a cyclic subgroup $H := \{e, x, x^2, \dots, x^{p-1}\}$ of order p. Necessarily $H \trianglelefteq G$ since $\frac{|G|}{|H|} = 2$ (by §3.3.4). Also, by Cauchy's Theorem, there exists an element y of order 2. Now $y \notin H$ (since no element of H has order 2), thus $H \neq Hy$ and so

$$G = H \cup Hy = \{e, x, x^2, \dots, x^{p-1}, y, xy, x^2y, \dots, x^{p-1}y\}.$$

Consider now the element yx. By Lagrange's Theorem, the order of yx is either $1, 2, p$ or $2p$. We claim that $o(yx) = 2$. Well certainly $o(yx) \neq 1$ since y cannot be the inverse of x (they have different orders), and certainly $o(yx) \neq 2p$ since then G would be cyclic (and so abelian). It remains to show that $o(yx) \neq p$. Suppose, for the aid of a contradiction, that $(yx)^p = e$. Consider the coset $H = He = H(yx)^p$. Now, $xH = H$ since $x \in H$, and so

$$Hyx = yxH = yH = Hy$$

where in the above manipulation we have used §3.3.2 since $H \trianglelefteq G$. By induction, it follows that $H(yx)^p = Hy^p$. But $y^2 = e$, so since p is odd, $y^p = y$. Hence

$$H = H(yx)^p = Hy^p = Hy,$$

which is a contradiction. It follows that $o(yx) = 2$. Now, since $y^2 = e$, we have

$$yxyx = e \implies yx = x^{-1}y^{-1} = x^{-1}y.$$

We claim that the relation $yx = x^{-1}y$, together with the relations $x^p = e$ and $y^2 = e$, completely determines the multiplication of all the elements in

$$G = H \cup Hy = \{e, x, x^2, \dots, x^{p-1}\} \cup \{y, xy, x^2y, \dots, x^{p-1}y\}$$

The key point is that, using the three relations, you can multiply any two elements in the set $\{e, x, x^2, \dots, x^{p-1}, y, xy, x^2y, \dots, x^{p-1}y\} = G$ and re-arrange to give another member of that set. For example

$$(x^2y)x = xxyx = xxx^{-1}y = xy \in \{e, x, x^2, \dots, x^{p-1}, y, xy, x^2y, \dots, x^{p-1}y\}.$$

(It is easy to check the general case.) Hence $G = \langle x, y \mid x^p = e, y^2 = e, yx = x^{-1}y \rangle$, which is D_p from §2.8. Hence $G \cong D_p$.

□

7.3. The finite quaternion group

7.3.1. *Theorem.* The 2×2 complex matrices

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

obey

$$I^2 = J^2 = K^2 = -1,\ IJ = -JI = K,\ JK = -KJ = I,\ KI = -IK = J.$$

7.3.2. *Theorem.* Let

$$Q = \{\pm 1, \pm I, \pm J, \pm K\} \subseteq \mathrm{SL}(2, \mathbb{C}).$$

Then Q is a subgroup of $\mathrm{SL}(2, \mathbb{C})$ (under matrix multiplication), and so in particular Q is a group of order 8.

Proof. Q is clearly nonempty. By the above relations, it is closed under multiplication. Further, ± 1 are their own inverse, and all the other elements have an inverse which is minus themselves (since $I(-I) = 1$ etc). Hence Q is closed under inverses. □

7.3.3. *Theorem.* Every nonabelian group of order 8 is isomorphic to either D_4 or Q.

Proof. See Problem 7.7 □

7.4. **Summary of small groups**

The list of all non-isomorphic groups of order ≤ 12 is as follows:

order	abelian groups	nonabelian groups
2	C_2	
3	C_3	
4	$C_4, C_2 \times C_2$	
5	C_5	
6	C_6	$S_3 \cong D_3$
7	C_7	
8	$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2$	D_4, Q
9	$C_9, C_3 \times C_3$	
10	C_{10}	D_5
11	C_{11}	
12	$C_{12}, C_2 \times C_6$	$D_6, A_4, \ldots$

The entries in the abelian column are clearly examples of that given order; they are all the abelian groups of that order by §7.1.4. There are no nonabelian groups of order 2, 3, 4, 5, 7, 9 and 11 by §7.2.1.

The entries in the nonabelian column are clearly examples of nonabelian groups of that given order. The nonabelian groups of orders 6 and 10 are all the nonabelian groups of that order by §7.2.2. The groups D_4 and Q are the only nonabelian groups of order 8 by Problem 7.7.

The only thing that still needs to be found is the number of nonabelian groups of order 12. It turns out that there are three in total.