Groups and Group Actions

Richard Earl

Hilary and Trinity Terms 2014

Syllabus

Hilary Term (8 lectures)

- Axioms for a group and for an Abelian group. Examples including geometric symmetry groups, matrix groups (GL_n, SL_n, O_n, SO_n, U_n), cyclic groups. Products of groups. [2]

- Permutations of a finite set under composition. Cycles and cycle notation. Order. Transpositions; every permutation may be expressed as a product of transpositions. The parity of a permutation is well-defined via determinants. Conjugacy in permutation groups. [2]

- Subgroups; examples. Intersections. The subgroup generated by a subset of a group. A subgroup of a cyclic group is cyclic. Connection with hcf and lcm. Bezout's Lemma. [1.5]

- Recap on equivalence relations including congruence $\bmod n$ and conjugacy in a group. Proof that equivalence classes partition a set. Cosets and Lagrange's Theorem; examples. The order of an element. Fermat's Little Theorem. [2.5]

Trinity Term (8 lectures)

- Isomorphisms, examples. Groups up to isomorphism of order 8 (stated without proof). Homomorphisms of groups with motivating examples. Kernels. Images. Normal subgroups. Quotient groups; examples. First Isomorphism Theorem. Simple examples determining all homomorphisms between groups. [3]

- Group actions; examples. Definition of orbits and stabilizers. Transitivity. Orbits partition the set. Stabilizers are subgroups. [2]

- Orbit-stabilizer Theorem. Examples and applications including Cauchy's Theorem and to conjugacy classes. [1]

- Orbit-counting formula. Examples. [1]

- The representation $G \to \mathrm{Sym}(S)$ associated with an action of G on S. Cayley's Theorem. Symmetry groups of the tetrahedron and cube. [1]

Recommended Texts

- M. A. Armstrong Groups and Symmetry (Springer, 1997)

STANDARD GROUP NOTATION

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ – the integers/rationals/reals/complex numbers under $+$.
- C_n – the cyclic group of order n.
- $\mathbb{Z}_n$ – the integers, modulo n, under $+$. ($\mathbb{Z}_n$ is isomorphic to C_n)
- $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ – non-zero rationals/reals/complex numbers under $\times$.
- $\mathbb{Z}_p^*$ – the non-zero elements of $\mathbb{Z}_p$, where p is a prime, under $\times$.
- $\mathbb{Z}_n^*$ – more generally for composite n, the units of $\mathbb{Z}_n$, those elements coprime with n under $\times$.
- $(0,\infty)$ – the positive real numbers under $\times$.
- $\mathrm{Sym}(S)$ – the permutations (i.e. bijections $S \to S$) of a set S under composition.
- S_n – permutations of $\{1, 2, \ldots n\}$ under composition.
- A_n – even permutations of $\{1, 2, \ldots, n\}$ under composition.
- D_{2n} – the symmetries of a regular n-sided polygon under composition.
- V or V_4 – the Klein four-group $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong \{e, (12)(34), (13)(24), (14)(23)\}$.
- Q_8 – the quaternion group $\{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$.
- S^1 – the complex numbers with unit modulus under multiplication.
- $GL(n, F)$ – invertible $n \times n$ matrices with entries in the field F under matrix multiplication.
- $SL(n, F)$ – the subgroup of $GL(n, F)$ whose elements have determinant 1.
- $AGL(n, F)$ – the affine maps of F^n.
- $O(n)$ – orthogonal $n \times n$ real matrices ($A^{-1} = A^T$) under matrix multiplication. Also $SO(n)$.
- $U(n)$ – unitary $n \times n$ complex matrices ($A^{-1} = \bar{A}^T$) under matrix multiplication. Also $SU(n)$.
- $\mathrm{Aut}(G)$ – the automorphisms (i.e. isomorphisms $G \to G$) of a group G under composition.
- $G_1 \times G_2$ – the (direct) product group of two groups G_1 and G_2.
- G/H – the quotient (or factor) group of a group G by a normal subgroup H of G.
- $\langle g \rangle$ – the cyclic subgroup of G generated by $g \in G$.
- $\langle S \rangle$ – the subgroup of a group G generated by a subset S of G.

1. THE GROUP AXIOMS

1.1 Abstraction

Abstract algebra began as a late nineteenth century construct bringing together many results and observations from the previous century. During the twentieth century, throughout much of pure mathematics, abstraction was to play an important role in shaping the subject. Prior to the nineteenth century, most mathematics had begun with some interest in real-world problems. Perhaps due to the paradigm-smashing discovery of non-euclidean geometries, nineteenth century mathematicians were more willing to cut that cord. In any case, thinking abstractly, mathematicians began looking at the underlying rules, logic and structures that drove seemingly disparate results. The power of abstraction, then, is its generality: beginning with the rules of an abstract structure, one can begin to demonstrate results that apply to all examples of that structure. Whilst the nature of a specific structure is likely grounded in some important concrete examples, the proof itself emerges independent of any particular examples. Still more, with luck, the proof will be that much more apparent as it focuses on the structure's rules only and there is no distraction from superficial clutter.

In this first course in abstract algebra we concentrate on *groups*. Groups, particularly in the form of "substitution groups", had been apparent in the work of Galois, Gauss, Cauchy, Abel et al. in the early nineteenth century. The general axioms for a group were first written down by Cayley in 1849, but their importance wasn't acknowledged at the time. Two other important algebraic structures are *rings* and *fields* – you will likely have met the field axioms in Linear Algebra I and Analysis I. Both these concepts are due to Richard Dedekind (1831-1916) who was arguably the father of abstract algebra; certainly he was one of the first to fully appreciate the power of abstract structures. Fields and rings naturally lead to examples of groups also. It wasn't until the 1870s that an appreciation of the merit of abstract structures was showing, especially in the nascent algebraic number theory which grew out of efforts to prove Fermat's Last Theorem.

1.2 Binary Operations

Definition 1 *A* ***binary operation*** $*$ *on a set* S *is a map* $*\colon S \times S \to S$. *We write* $a * b$ *for the image of* (a, b) *under* $*$.

So a binary operation takes two inputs a, b from S in a given order and returns a single output $a * b$ which importantly has to be in S. Standard examples include addition, multiplication and composition but there are many other examples as well.

Example 2 *The following are examples of binary operations.*

(i) $+, -, \times$ *on* $\mathbb{R}$*;* $\div$ *is not a binary operation on* $\mathbb{R}$ *as, for example* $1 \div 0$ *is undefined;*

(ii) $\wedge$*, the cross product, on* $\mathbb{R}^3$*;*

(iii) min *and* max *on* $\mathbb{N}$*;*

(iv) $\circ$*, composition, on the set* $\mathrm{Sym}(S)$ *of bijections of a set* S *to itself;*

(v) matrix multiplication on the set of $n \times n$ *complex invertible matrices (for a given* n*).*

Definition 3 *A binary operation* $*$ *on a set* S *is said to be* ***associative*** *if, for any* $a, b, c \in S$*,*

$$(a * b) * c = a * (b * c)\,.$$

In particular, this means an expression such as $a_1 * a_2 * \cdots * a_n$ *always yields the same result, irrespective of how the individual parts of the calculation are performed.*

Definition 4 *A binary operation* $*$ *on a set* S *is said to be* ***commutative*** *if, for any* $a, b \in S$*,*

$$a * b = b * a.$$

Definition 5 *An element* $e \in S$ *is said to be an* ***identity element*** *(or simply an* ***identity****) for an operation* $*$ *on* S *if, for any* $a \in S$*,*

$$e * a = a = a * e.$$

Proposition 6 *Let* $*$ *be a binary operation on a set* S *and let* $a \in S$*. If an identity* e *exists then it is unique.*

Proof. Suppose that e_1 and e_2 are two identities for $*$. Then

$$\begin{array}{rcll} e_1 * e_2 & = & e_1 & \quad \text{as } e_2 \text{ is an identity;} \\ e_1 * e_2 & = & e_2 & \quad \text{as } e_1 \text{ is an identity.} \end{array}$$

Hence $e_1 = e_2$. ■

Definition 7 *If an operation* $*$ *on a set* S *has an identity* e *and* $a \in S$*, then we say that* $b \in S$ *is an* ***inverse*** *of* a *if*

$$a * b = e = b * a.$$

Proposition 8 *Let* $*$ *be an associative binary operation on a set* S *with an identity* e *and let* $a \in S$*. Then an inverse of* a*, if it exists, is unique.*

Proof. Suppose that b_1 and b_2 are inverses of a. Then

$$\begin{array}{rcl} b_1 * (a * b_2) & = & b_1 * e = b_1; \\ (b_1 * a) * b_2 & = & e * b_2 = b_2. \end{array}$$

By associativity $b_1 = b_2$. ■

Notation 9 *If $*$ is an associative binary operation on a set S with identity e, then the inverse of a (if it exists) is written a^{-1}.*

Example 10 *If we look at the binary operations in Example 2 then we note:*
(i) $+$ on $\mathbb{R}$ is associative, commutative, has identity 0 and $x^{-1}\colon = -x$ for any x;
$-$ on $\mathbb{R}$ is not associative or commutative and has no identity;
$\times$ on $\mathbb{R}$ is associative, commutative, has identity 1 and $x^{-1}\colon = 1/x$ for any nonzero x.
(ii) $\wedge$ on $\mathbb{R}^3$ is not associative or commutative and has no identity;
(iii) $\min$ on $\mathbb{N}$ is both associative and commutative but has no identity;
$\max$ on $\mathbb{N}$ is both associative and commutative and has identity 0 (being the least element of $\mathbb{N}$) though no positive integer has an inverse;
(iv) $\circ$ is associative, but not commutative, with the identity map $x \mapsto x$ being the identity element and as permutations are bijections they each have inverses;
(v) matrix multiplication on $n \times n$ invertible complex matrices is associative, but not commutative, with identity element I_n and $A^{-1}\colon = A^{-1}$ (unsurprisingly).

Remark 11 *Given a binary operation $*$ on S and a subset $T \subseteq S$, then we have a restriction $*\colon T \times T \to S$ which need not generally be a binary operation on T. We will, quite naturally, be interested in those subsets T for which $*$ restricts to a binary operation $*\colon T \times T \to T$ on T. In this case, T is said to be **closed** under $*$.*

Example 12 *$+$ is a binary operation on $\mathbb{Z}$.*
(i) Let $m \in \mathbb{Z}$. The set $m\mathbb{Z} = \{mn\colon n \in \mathbb{Z}\}$ is closed with a identity 0 and inverses.
(ii) The set $\{n \in \mathbb{Z}\colon n \geqslant 1\}$ is closed under $+$ but has no identity nor inverses.

1.3 The Group Axioms

Definition 13 *A **group** $(G, *)$ consists of a set G and a binary operation $*$ on G*

$$*\colon G \times G \to G, \qquad (a, b) \mapsto a * b$$

such that
(i) $*$ is associative – that is $a * (b * c) = (a * b) * c$ for any $a, b, c \in G$;
(ii) there is an identity e which satisfies $e * a = a = a * e$ for all $a \in G$;
(iii) for each $a \in G$ there exists an inverse a^{-1} such that $a * a^{-1} = e = a^{-1} * a$.

Remark 14 *If the operation $*$ is clear and unambiguous then we will often simply say "G is a group" as a shorthand for "$(G, *)$ is a group".*

Remark 15 *When verifying that $(G, *)$ is a group we have to check (i), (ii), (iii) above and **also** that $*$ is a binary operation – that is, $a * b \in G$ for all $a, b, \in G$; this is sometimes referred to as **closure.***

Notation 16 *It is common notation to suppress the binary operation $*$ when discussing groups generally and instead to write ab for $a * b$. We shall do this from now on.*

Notation 17 *Also, when n is an integer, we will write*

$$a^n = \begin{cases} \underbrace{aaa \cdots a}_{n \text{ times}} & n > 0; \\ e & n = 0; \\ \underbrace{a^{-1}a^{-1} \cdots a^{-1}}_{-n \text{ times}} & n < 0. \end{cases}$$

Basic rules of algebra following from the group axioms are:

Proposition 18 *Let G be a group, $x, y, z \in G$ and $m, n \in \mathbb{Z}$. Then*
(a) $(xy)^{-1} = y^{-1}x^{-1}$.
(b) $(x^n)^{-1} = x^{-n}$.
(c) $x^m x^n = x^{m+n}$.
(d) $(x^m)^n = x^{mn}$.
(e) (Cancelling on the left) If $xy = xz$ then $y = z$.
(f) (Cancelling on the right) If $xy = zy$ then $x = z$.

Proof. Left as exercises. ■

Definition 19 *We say that a group G is* ***abelian,*** *after the Norwegian mathematician Niels Abel (1802-1829), if the group operation is commutative – that is,*

$$g_1 g_2 = g_2 g_1 \quad \text{for all } g_1, g_2 \in G.$$

Example 20 *The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ form abelian groups under $+$ with $e = 0$ and $x^{-1} \colon = -x$ in each case.*

Example 21 *The sets $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$ $\mathbb{C}\backslash\{0\}$ form abelian groups under $\times$ with $e = 1$ and $x^{-1} \colon = 1/x$ in each case. These groups are respectively denoted as $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$.*

Remark 22 *More generally if $(F, +, \times)$ is a field then $(F, +)$ and $(F\backslash\{0\}, \times)$ are both abelian groups.*

Example 23 *The set of positive real numbers $(0, \infty)$ form an abelian group under $\times$ with $e = 1$ and $x^{-1} \colon = 1/x$.*

Example 24 *Any vector space forms an abelian group under $+$.*

Example 25 *Show that the $n \times n$ invertible real matrices form a group under matrix multiplication. This group is denoted $GL(n, \mathbb{R})$ and is called the n**th general linear group**.*

Show that $GL(n, \mathbb{R})$ is non-abelian when $n > 1$.

Solution. Our operation, matrix multiplication, is a binary operation because if A and B are invertible $n \times n$ real matrices then AB is invertible with $(AB)^{-1} = B^{-1}A^{-1}$.

Matrix multiplication is associative.

The group has an identity I_n as $I_nA = AI_n = A$ for all A and I_n is invertible.

Every element $A \in GL(n,\mathbb{R})$ has an inverse A^{-1} (in the usual sense) which is invertible as $(A^{-1})^{-1} = A$ and which satisfies $AA^{-1} = A^{-1}A = I_n$.

If $n \geqslant 2$ then we see that

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & I_{n-2} \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & I_{n-2} \end{pmatrix}$$

don't commute as $(AB)_{11} = 2 \neq 1 = (BA)_{11}$ and hence $GL(n,\mathbb{R})$ is non-abelian. ■

There are other important matrix groups. Let n be a positive integer.

Example 26 *The real invertible $n \times n$ matrices with determinant 1 form a group $SL(n,\mathbb{R})$ (the **special linear group**) under matrix multiplication which is non-abelian for $n \geqslant 2$.*

Example 27 *The orthogonal $n \times n$ matrices form a group $O(n)$ under matrix multiplication which is non-abelian for $n \geqslant 2$. (Recall a real matrix A is orthogonal if $A^{-1} = A^T$.)*

Example 28 *The orthogonal $n \times n$ matrices with determinant 1 form a group $SO(n)$ under matrix multiplication which is non-abelian for $n \geqslant 3$.*

Definition 29 *A complex square matrix A is called **unitary** if $A^{-1} = \overline{A}^T$, that is the transpose of the conjugate of A.*

Example 30 *Show that the unitary $n \times n$ matrices form a group $U(n)$ under matrix multiplication which is non-abelian for $n \geqslant 2$.*

Solution. This is left to Exercise Sheet 1, Question 3. ■

Example 31 *The set $S^1 = \{z \in \mathbb{C}\colon |z| = 1\}$ forms an abelian group under multiplication. Note that the three groups S^1, $U(1)$, $SO(2)$ can all be naturally identified by*

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

An important (if rather elementary) family of groups is the *cyclic groups.*

Definition 32 *A group G is called **cyclic** if there exists $g \in G$ such that*

$$G = \left\{g^k \colon k \in \mathbb{Z}\right\}.$$

*Such a g is called a **generator**. As $g^ig^j = g^{i+j} = g^jg^i$ then cyclic groups are abelian.*

Example 33 *$\mathbb{Z}$ is cyclic and has generators 1 and -1.*

Example 34 *Let $n \geqslant 1$. The* n**th cyclic group** C_n *is the group with elements*

$$\{e, g, g^2, \ldots, g^{n-1}\}$$

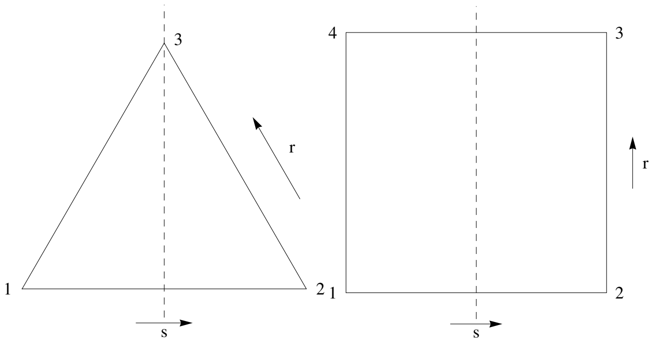
which satisfy $g^n = e$. So given two elements in C_n we define

$$g^i * g^j = \begin{cases} g^{i+j} & \text{if } 0 \leqslant i+j < n, \\ g^{i+j-n} & \text{if } n \leqslant i+j \leqslant 2n-2. \end{cases}$$

Another important family of groups is the *dihedral groups*.

Example 35 ***(The Dihedral Groups)*** *Let $n \geqslant 3$ be an integer and consider a regular n-sided polygon P in the plane. We then write D_{2n} for the set of isometries of the plane which map the polygon back to itself. It is clear that D_{2n} forms a group under composition as (i) the identity map is in D_{2n}, (ii) the product of two isometries taking P to P is another such isometry, (iii) the inverse of such an isometry is another such isometry, (iv) composition is associative. Here "D" stands for "dihedral", meaning two-sided.*

We consider the $n = 3$ or D_6 case first, that is where the polygon is an equilateral triangle as in the first diagram below.



$n = 3$ $n = 4$

We will denote rotation anticlockwise by $2\pi/3$ as r and denote reflection in the vertical as s. We will also label the vertices as $1, 2, 3$. It is easy to see that the following symmetries are all different

$$e, \quad r, \quad r^2, \quad s, \quad rs, \quad r^2 s.$$

One way of seeing this is by noting how these symmetries permute the vertices; note that these six symmetries respectively permute the vertices as

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

In fact, these are the only symmetries of the triangle as there are $6 = 3!$ permutations of the vertices.

When $n = 4$ (i.e. when the group is D_8) we will similarly denote rotation anticlockwise by $\pi/2$ as r and again denote reflection in the vertical as s. If we will label the vertices as

1, 2, 3, 4 *then we note that the following eight symmetries are distinct because of their effect on the vertices:*

$$
\begin{aligned}
e &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad r^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad r^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \\
s &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad rs = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad r^2 s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad r^3 s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.
\end{aligned}
$$

What is slightly unclear in this case is whether there are any further symmetries. Clearly some permutations of the vertices cannot be performed as symmetries – for example, swapping just 3 *and* 4 *is not possible as, afterwards,* 1 *and* 3 *would no longer be opposite one another on a diagonal. We shall see in Proposition 36 that the eight symmetries above are indeed the only possible symmetries of the square.*

Proposition 36 *Let P be a regular n-sided polygon P in the plane with r denoting anticlockwise rotation through $2\pi/n$ about P's centre and s denoting reflection in an axis of P. Then the symmetries of P are*

$$e, r, r^2, \ldots r^{n-1}, s, rs, r^2 s, \ldots r^{n-1} s. \tag{1.1}$$

Proof. Label the vertices of P as $1, 2, \ldots, n$ in an anticlockwise order. Let t be a symmetry of P. Once t has been effected then the vertices will either read $1, 2, \ldots n$ anticlockwise or clockwise. Suppose the former and say that 1 has moved to position k where $1 \leqslant k \leqslant n$. Then $r^{1-k}t$ returns 1 to position 1 and – more generally, as the vertices are in an anticlockwise order – all vertices to their original starting positions. Hence $r^{1-k}t = e$ and we see $t = r^{k-1}$. If instead t changes the vertices to a clockwise order then ts – as s flips the polygon – keeps them in an anticlockwise order. As before we see that $ts = r^{k-1}$ for some $1 \leqslant k \leqslant n$ and hence $t = r^{k-1}s$ as $s^{-1} = s$.

Hence the symmetries in (1.1) are the only possible. To see that these $2n$ symmetries are distinct, well firstly each of $e, r, r^2, \ldots r^{n-1}$ keep the vertices in the same anticlockwise order but each moves vertex 1 to a different place, and each of $s, rs, r^2 s, \ldots r^{n-1}s$ reverses the order of the vertices and each moves vertex 1 to a different position. ■

Given two groups G and H, there is a natural way to make their Cartesian product $G \times H$ into a group. Recall that as a set

$$G \times H = \{(g, h) \colon g \in G, h \in H\}.$$

We then define the *product group* $G \times H$ as follows.

Theorem 37 *Let $(G, *_G)$ and $(H, *_H)$ be groups. Then the operation $*$ defined on $G \times H$ by*

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

is a group operation. $(G \times H, *)$ is called the ***product group*** *or the* ***product of*** *G and H.*

Proof. As $*_G$ and $*_H$ are both associative binary operations then it follows easily from the definition to see that $*$ is also an associative binary operation on $G \times H$. We also note

$$e_{G\times H} = (e_G, e_H) \ \text{ and } \ (g,h)^{-1} = (g^{-1}, h^{-1})$$

as for any $g \in G, h \in H$

$$\begin{aligned} (e_G, e_H) * (g,h) &= (g,h) = (g,h) * (e_G, e_H); \\ (g^{-1}, h^{-1}) * (g,h) &= (e_G, e_H) = (g,h) * (g^{-1}, h^{-1}). \end{aligned}$$

■

Definition 38 *The cardinality $|G|$ of a group G is called the* **order** *of G. We say that a group G is* **finite** *if $|G|$ is finite.*

One way to represent a finite group is by means of the *group table* or *Cayley table* (after the English mathematician Arthur Cayley, 1821-1895).

Definition 39 *Let $G = \{e, g_2, g_3, \ldots, g_n\}$ be a finite group. The* **Cayley table** *(or* **group table***) of G is a square grid which contains all the possible products of two elements from G. The product $g_i g_j$ appears in the ith row and jth column of the Cayley table*

Remark 40 *Note that a group is abelian if and only if its Cayley table is symmetric about the main (top-left to bottom-right) diagonal.*

Example 41 *The Cayley table of D_6 is given below*

$*$	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

All these product can be worked out from just the three rules

$$r^3 = e, \qquad s^2 = e, \qquad sr = r^2 s.$$

So, for example, we see

$$\left(r^2 s\right)(rs) = r^2 (sr)\, s = r^2 \left(r^2 s\right) s = r^4 s^2 = r.$$

Proposition 42 *A Cayley group table is a latin square. That is, every group element appears precisely once in each row and in each column.*

Proof. Given a particular group element g_k we see that the map $G \to G$ given by $g \mapsto g_k g$ is a bijection with inverse $g \mapsto g_k^{-1} g$. This means that the kth row contains each element of G precisely once. Likewise the map $G \to G$ given by $g \mapsto g g_k$ is a bijection with inverse $g \mapsto g g_k^{-1}$, and this means that the kth column contains each element of G precisely once. ■

Example 43 *Note that, in both D_6 and D_8, the rotations by themselves – so $\{e, r, r^2\}$ when $n = 3$ and $\{e, r, r^2, r^3\}$ when $n = 4$ – make groups in their own rights. Their group tables are given below.*

$*$	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^r	e	r

,

$*$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

We can see that these groups are the cyclic groups C_3 and C_4.

Put another way this means that $\{e, r, r^2\}$ is a subgroup of D_6 and $\{e, r, r^2, r^3\}$ is a subgroup of D_8.

Definition 44 *Let G be a group. We say that a subset $H \subseteq G$ is a* ***subgroup*** *of G if the group operation $*$ restricts to make a group of H. That is H is a subgroup of G if:*

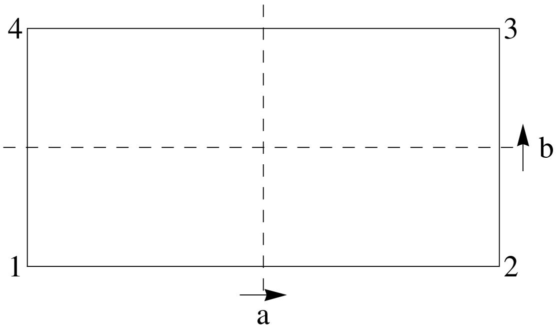
(i) $e \in H$;

(ii) whenever $g_1, g_2 \in H$ then $g_1 g_2 \in H$.

(iii) whenever $g \in H$ then $g^{-1} \in H$.

Note that there is no need to require that associativity holds for products of elements in H as this follows from the associativity of products in G.

Example 45 *If we consider the symmetry group of a (non-square) rectangle, then two symmetries are reflection in the vertical, which we will denote a, and reflection in the horizontal, which we will denote b. A further symmetry is ab which is rotation by π; we will write $c = ab$.*



If we label the vertices of the rectangle as $1, 2, 3, 4$ then we identify e, a, b, c as

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

These are in fact the only symmetries of the rectangle. To see this we only have to consider the position of vertex 1 after a symmetry has been effected; once we know where 1 has moved to then the positions of the remaining vertices are uniquely determined by the rectangle's geometry. The Cayley table for this group is then

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Note that the group is abelian.

This group – whether thought of in terms of the symmetries of a rectangle or considered as permutations – is often called the ***Klein four-group,*** *after the German mathematician Felix Klein (1849-1925) and denoted* V *or* V_4*. (The* V *stands for "vier", the German for "four".)*

Example 46 ***Groups of order four or less.*** *What ways are there to fill a Cayley table for a group of order* $n \leqslant 4$*? We will always have an identity element* e *and we will label the remaining element* $a, b, c, \ldots$ *depending on the order of the group.*

In the case $n = 1$*, there is clearly only one such table.*

When $n = 2$ *then the products* e^2, ea, ae *are all clear from the group axioms; further for the table to be a latin square we also need that* $a^2 = e$*.*

When $n = 3$ *then the products* e^2, ea, ae, be, eb *are all clear from the group axioms. Further we see that* ab *can be neither* a *nor* b *if the table is to form a latin square. The only remaining possibility is that* $ab = e$ *and likewise that* $ba = e$*. From there, the remainder of the table is uniquely determined on the basis of it being a latin square.*

$*$	e
e	e

,

$*$	e	a
e	e	a
a	a	e

,

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

.

The $n = 4$ *situation is slightly more complicated. If we consider* ba *then it can (potentially) be either* e *or* c*.*

Case (i): if $ba = e$ *then* $b = a^{-1}$ *and so* $ab = e$ *also. (See first table below). But then, focusing on the third row and column, we must also have* $bc = a = cb$ *and* $b^2 = c$*. (See the second table below.) Finally, looking at the second row, we see that* $a^2 = c$ *and* $ca = b = ac$ *and* $c^2 = e$ *is the only remaining possibility. See final table.*

$*$	e	a	b	c
e	e	a	b	c
a	a	?	e	?
b	b	e	?	?
c	c	?	?	?

,

$*$	e	a	b	c
e	e	a	b	c
a	a	?	e	?
b	b	e	c	a
c	c	?	a	?

,

$*$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

But is this a genuine group table? Note, in this case, that $c = a^2$ *and* $b = a^3$*. If we swap the* b *and* c *rows and columns, we rewrite this table as*

$*$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

which we have already seen as a concrete example of a group, namely the four rotations of a square.

Case (ii) Instead now we consider the case $ba = c$*. As* $ab \neq e$ *then* $ab = c$ *is the only remaining possibility. (See table below.) At this point, though, the way forward is still not* *clear, in the sense that we can continue to create a latin square in different ways. We could (potentially) have $a^2 = b$ or $a^2 = e$.*

$*$	e	a	b	c
e	e	a	b	c
a	a	?	c	?
b	b	c	?	?
c	c	?	?	?

.

Case (ii)(a) Assuming $ba = c$ and $a^2 = b$ then we can complete the table (See first table below). But if we note $b = a^2$ and $c = a^3$ then we see we in fact have reproduced the same table as in case (i).

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

,

$*$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

Cases (ii)(b') and (ii)(b") If we assume $ba = c$ and $a^2 = e$ then we can only complete the table as far as the first table below. We could still have either (b') $b^2 = a$ (see second table) or (b") $b^2 = e$ (see third table).

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	?	?
c	c	b	?	?

,

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

,

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

.

The second table again is nothing new as $a = b^2$, $c = b^3$, so that this is in fact the same group as we have just met twice already. But the final table is fundamentally different, for example as every element is self-inverse. We recognise it as the symmetry group of the rectangle or the Klein group V_4 that we met previously.

Remark 47 *In all, then, there are four latin squares of size 4×4 with rows and columns (e, a, b, c). In each case, the latin square represented a group though this is not always the case (see Exercise Sheet 1, Question 2).*

To make the following discussion a little easier we introduce now the idea of the *order* of a group element.

Definition 48 *Let G be a group and $g \in G$. The* **order** *of g, written $\mathrm{o}(g)$, is the least positive integer r such that $g^r = e$. If no such integer exists then we say that g has infinite order.*

Remark 49 *Note, now, that there are unfortunately two different uses of the word order: the order of a group is the number of elements it contains; the order of a group element is the least positive power of that element which is the identity.*

In the above we have seen that *in essence* there is one group of order one, one of order two, one of order three and two of order four. Though the symbols for the elements may vary, an order two group consists of an identity element and an element of order two – so that it is in essence C_2; an order three group consists of an identity, an element of order three and its square – so that it is in essence C_3; an order four group either consists of an identity, an element of order four, its square and cube – so that is in essence C_4 – or it consists of an identity and three distinct elements of order two which commute – so that it is essentially V_4.

The idea which rigorously captures the idea of "in essence" is that of the *isomorphism.* For two groups to be the same "in essence" means that, suitably relabelled, their Cayley tables would be the same. That relabelling would be an isomorphism.

Definition 50 *An* ***isomorphism*** $\phi\colon G \to H$ *between two groups* $(G, *_G)$ *and* $(H, *_H)$ *is a bijection such that for any* $g_1, g_2 \in G$ *we have*

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2).$$

Two groups are said to be ***isomorphic*** *if there is an isomorphism between them. Being isomorphic is fairly easily seen to be an equivalence relation. There may well be more than one isomorphism between isomorphic groups.*

The Cayley tables of two isomorphic groups would in essence be the same as follows. If $\phi\colon G \to H$ is an isomorphism and $G = \{g_1, \ldots g_n\}$ so that $H = \{\phi(g_1), \ldots, \phi(g_n)\}$ then ϕ would set up the following correspondence between the Cayley tables of G and H

$*_G$	g_1	$\cdots$	g_j	$\cdots$	g_n
g_1					
$\vdots$					
g_i			$g_i *_G g_j$		
$\vdots$					
g_n					

$\xrightarrow{\phi}$

$*_H$	$\phi(g_1)$	$\cdots$	$\phi(g_j)$	$\cdots$	$\phi(g_n)$
$\phi(g_1)$					
$\vdots$					
$\phi(g_i)$			$\phi(g_i) *_H \phi(g_j)$		
$\vdots$					
$\phi(g_n)$					

so that if the two tables are to properly correspond under ϕ we need to have in each case

$$\phi(g_i *_G g_j) = \phi(g_i) *_H \phi(g_j).$$

Remark 51 *We have seen that there are, up to isomorphism,* $1, 1, 1, 2$ *groups of order* $1, 2, 3, 4$ *respectively. In general it is a very difficult problem to work out how many groups there are of a given order. The number of different groups g for each order n up to* 80 *are given in the table below.*

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
g	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1	5
n	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
g	2	2	1	15	2	2	5	4	1	4	1	51	1	2	1	14	1	2	2	14
n	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
g	1	6	1	4	2	2	1	52	2	5	1	5	1	15	2	13	2	2	1	13
n	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
g	1	2	4	267	1	4	1	5	1	4	1	50	1	2	3	4	1	6	1	52

2. PERMUTATION GROUPS

Definition 52 *Let S be a set. A bijection $S \to S$ is called a* **permutation** *of S and the set of permutations of S is denoted* $\mathrm{Sym}(S)$.

If n is a positive integer, then we write S_n for $\mathrm{Sym}(\{1, 2, \ldots n\})$.

Notation 53 ***Important:*** *though this convention is not universal, in Oxford it is usual to write permutations on the right. So for $k \in \{1, 2, \ldots, n\}$ and $\sigma, \tau \in S_n$ then we would write $k\sigma$ for $\sigma(k)$ and $k\sigma\tau$ for $\tau(\sigma(k))$. So the permutation $\sigma\tau$ is the composition of σ first with τ second.*

Theorem 54 *Let S be a set.*
(a) Then $\mathrm{Sym}(S)$ *forms a group under composition. It is called the* ***symmetry group*** *of S.*
(b) If $|S| \geqslant 3$ then $\mathrm{Sym}(S)$ *is non-abelian.*
(c) The cardinality of S_n is $n!$

Proof. (a) We know that the composition of two bijections is a bijection. So $\circ$ is indeed a binary operation on $\mathrm{Sym}(S)$. Further for any $f, g, h \in \mathrm{Sym}(S)$ and $x \in S$ we have

$$x\left((fg)\,h\right) = \left(x\,(fg)\right)h = \left((xf)\,g\right)h = (xf)\,(gh) = x\left(f\,(gh)\right)$$

So $\circ$ is an associative binary operation. The identity of $\mathrm{Sym}(S)$ is easily seen to be the identity map

$$id_S(x) = x \qquad \text{for all } x \in S$$

and the inverse of $f \in \mathrm{Sym}(S)$ is, unsurprisingly, its inverse map f^{-1}.

(b) If x_1, x_2, x_3 are three distinct elements of S then we can define two permutations of S by

$$\begin{aligned} f\colon x_1 &\mapsto x_1, \quad x_2 \mapsto x_3, \quad x_3 \mapsto x_2, \quad x \mapsto x \text{ for other } x; \\ g\colon x_1 &\mapsto x_2, \quad x_2 \mapsto x_1, \quad x_3 \mapsto x_3, \quad x \mapsto x \text{ for other } x; \end{aligned}$$

which do not commute as

$$\begin{aligned} fg\colon x_1 &\mapsto x_2, \quad x_2 \mapsto x_3, \quad x_3 \mapsto x_1, \quad x \mapsto x \text{ for other } x. \\ gf\colon x_1 &\mapsto x_3, \quad x_2 \mapsto x_1, \quad x_3 \mapsto x_2, \quad x \mapsto x \text{ for other } x; \end{aligned}$$

(c) For $f \in S_n$ there are n possibilities for $1f$, but as f is 1-1, and so $1f \neq 2f$, there are $n-1$ possibilities for $2f$ once $1f$ is known and likewise $n-2$ possibilities for $3f$ etc. In all then there are

$$n \times (n-1) \times (n-2) \times \cdots \times 1 = n!$$

permutations of $\{1, 2, \ldots, n\}$. ■

One (slightly cumbersome) way of writing down a permutation $\sigma \in S_n$ is as an array

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1\sigma & 2\sigma & 3\sigma & \cdots & n\sigma \end{pmatrix}$$

though we shall improve on this notation with the introduction of *cycle notation.*

Example 55 *(i) So S_2 is a group of order two which contains the elements*

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

The first element is the identity and the second is self-inverse.

(ii) And S_3 is a group of order six with contains the elements

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

The first element is e. If we write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

then we see (amongst other things) that

$$\begin{aligned}
\sigma^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \\
\sigma^3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e; \\
\tau^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = e; \\
\sigma\tau &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; \\
\tau\sigma^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.
\end{aligned}$$

The six elements of S_3 are in fact

$$e, \qquad \sigma, \qquad \sigma^2, \qquad \tau, \qquad \sigma\tau, \qquad \sigma^2\tau.$$

The Cayley table for S_3 is

$*$	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	e	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	e	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	e	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	e

Remark 56 *Note that the six permutations listed above as the elements of S_3 are the same as those listed in Example 35 and the above Cayley table for S_3 is identical to that in Example 41 once σ, τ are replaced with r, s. This shows that D_6 and S_3 are in fact isomorphic.*

Example 57 *Set*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \qquad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix},$$

in S_5. Determine the product $\alpha\beta\gamma$, the inverse of β and the order of γ.

Solution. We have

$$\begin{aligned}
\alpha\beta\gamma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}; \\
\beta^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 4 & 5 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}; \\
\gamma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}, \quad \gamma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}, \quad \gamma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}, \\
\gamma^5 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}, \quad \gamma^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e,
\end{aligned}$$

so that the order of γ is 6. ■

There is a special type of permutation, a *cycle*, which shall prove useful as we shall see that any permutation can be (essentially) uniquely decomposed as a product of cycles.

Definition 58 *A permutation $\sigma \in S_n$ is a* ***cycle*** *if there are distinct elements $a_1, a_2, \ldots, a_k$ in $\{1, 2, \ldots, n\}$ such that*

$$a_i\sigma = a_{i+1} \qquad \text{for } 1 \leqslant i < k; \qquad\qquad a_k\sigma = a_1;$$

and

$$x\sigma = x \qquad \text{for } x \notin \{a_1, a_2, \ldots, a_k\}.$$

The ***length*** *of such a cycle is k and we would refer to σ as a k-**cycle.** Note that the order of a k-cycle is k.*

Notation 59 ***Cycle notation:*** *We denote the above cycle as*

$$(a_1\, a_2\, a_3\, \cdots\, a_k).$$

Note that this notation isn't unique (in fact there are k such expressions in all) and that we have

$$(a_1\, a_2\, a_3\, \cdots\, a_k) = (a_2\, a_3\, a_4\, \cdots\, a_k\, a_1) = \cdots = (a_k\, a_1\, a_2\, \cdots\, a_{k-1}).$$

Example 60 *Note that α, β, γ, from Example 57 can be written as*

$$\alpha = (124), \qquad \beta = (13524), \qquad \gamma = (125)(34).$$

So α is a 3-cycle, β is a 5-cycle and γ is not a cycle.

Definition 61 *Two cycles $(a_1 \ldots a_k)$ and $(b_1 \ldots b_l)$ are said to be* ***disjoint*** *if $a_i \neq b_j$ for all i, j.*

Proposition 62 *Disjoint cycles commute.*

Proof. Let $\alpha = (a_1 \ldots a_k)$ and $\beta = (b_1 \ldots b_l)$. Then

$$\begin{array}{lll}
a_i\alpha\beta = a_{i+1}\beta = a_{i+1}, & a_i\beta\alpha = a_i\alpha = a_{i+1}, & \text{for } i < k; \\
a_k\alpha\beta = a_1\beta = a_1, & a_k\beta\alpha = a_k\alpha = a_1; & \\
b_i\alpha\beta = b_i\beta = b_{i+1}, & b_i\beta\alpha = b_{i+1}\alpha = b_{i+1}, & \text{for } i < l; \\
b_l\alpha\beta = b_l\beta = b_1, & b_l\beta\alpha = b_1\alpha = b_1; & \\
x\alpha\beta = x\beta = x, & x\beta\alpha = x\alpha = x, & \text{for } x \notin \{a_1, \ldots, a_k, b_1, \ldots, b_l\}.
\end{array}$$

■

Theorem 63 *Every permutation can be written as a product of disjoint cycles. This expression is unique up to the cycling of elements within cycles and permuting the order of the cycles.*

Proof. Let $\sigma \in S_n$ and let $a_1 \in \{1, 2, \ldots, n\}$. Consider the sequence

$$a_1,\ a_1\sigma,\ a_1\sigma^2,\ a_1\sigma^3, \ldots$$

As the elements of the sequence are in the set $\{1, 2, \ldots n\}$ then the sequence must have repetitions so that $a_1\sigma^i = a_1\sigma^j$ for some $i < j$. But then $a_1\sigma^{j-i} = a_1$ is an earlier repetition of a_1 and we see that a_1 is in fact the first element of the sequence to repeat. Say $a_1\sigma^{k_1} = a_1$ is the first repetition of a_1. We see then that

$$\sigma \text{ acts on the set } \left\{a_1, a_1\sigma, a_1\sigma^2, \ldots, a_1\sigma^{k_1-1}\right\} \text{ as the cycle } \left(a_1\, a_1\sigma\, a_1\sigma^2 \ldots a_1\sigma^{k_1-1}\right).$$

The set $\left\{a_1, a_1\sigma, a_1\sigma^2, \ldots, a_1\sigma^{k_1-1}\right\}$ is called the *orbit* of a_1.

If $k_1 = n$ then σ is a cycle and we are done. If not then we take a second element a_2 not in the orbit of a_1 and we can similarly see that σ acts as a second cycle on the orbit of a_2. These orbits are disjoint for if $a_1\sigma^i = a_2\sigma^j$ for some i, j then $a_2 = a_1\sigma^{i-j}$ and we see that a_2 was in the orbit of a_1, a contradiction. As the set $\{1, 2, \ldots, n\}$ is finite then these orbits eventually exhaust the set and we see that

$$\sigma = \left(a_1\, a_1\sigma\, a_1\sigma^2 \ldots a_1\sigma^{k_1-1}\right)\left(a_2\, a_2\sigma\, a_2\sigma^2 \ldots a_2\sigma^{k_2-1}\right) \cdots \left(a_r\, a_r\sigma\, a_r\sigma^2 \ldots a_1\sigma^{k_r-1}\right)$$

where r was the number of different orbits.

Suppose now that

$$\sigma = \rho_1\rho_2 \cdots \rho_k = \tau_1\tau_2 \cdots \tau_l$$

are expressions for σ as products of disjoint cycles. Then 1 appears in precisely one cycle ρ_i and in precisely one cycle τ_j. By reordering the appearances of the cycles if necessary (as they do commute, being disjoint) we may assume that 1 appears in ρ_1 and τ_1. By cycling the elements of the cycles ρ_1 and τ_1, if necessary, we may assume that 1 appears at the start of each cycle. Hence we see

$$\rho_1 = \left(1\, 1\sigma\, 1\sigma^2 \cdots 1\sigma^{k-1}\right) = \tau_1$$

where k is the size of the orbit of 1. By continuing similarly with an element not in the orbit of 1 we can show (with permitted permuting of cycles and cycling within cycles) that $\rho_2 = \tau_2$ etc. to complete the proof. ■

Definition 64 *As a consequence of the above theorem, the lengths of the various cycles of a permutation and the number of cycles of each such length, is well-defined. The is known as the* ***cycle decomposition type*** *(or just* ***cycle type****) of the permutation.*

Example 65 *Write the following permutations in S_9 as products of disjoint cycles.*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 9 & 7 & 3 & 2 & 4 & 8 & 1 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 7 & 5 & 1 & 3 & 6 & 2 & 8 \end{pmatrix}.$$

Write α^{-1} and β^{272} as products of disjoint cycles.

Solution. We see that

$$1 \xrightarrow{\alpha} 5 \xrightarrow{\alpha} 3 \xrightarrow{\alpha} 9 \xrightarrow{\alpha} 1, \qquad 2 \xrightarrow{\alpha} 6 \xrightarrow{\alpha} 2, \qquad 4 \xrightarrow{\alpha} 7 \xrightarrow{\alpha} 4, \qquad 8 \xrightarrow{\alpha} 8$$

and so

$$\alpha = (1539)\,(26)\,(47)\,(8)\,.$$

Hence we also see

$$\alpha^{-1} = (1935)\,(26)\,(47)\,(8)\,.$$

We also see

$$1 \xrightarrow{\beta} 4 \xrightarrow{\beta} 5 \xrightarrow{\beta} 1, \qquad 2 \xrightarrow{\beta} 9 \xrightarrow{\beta} 8 \xrightarrow{\beta} 2, \qquad 3 \xrightarrow{\beta} 7 \xrightarrow{\beta} 6 \xrightarrow{\beta} 3,$$

so that

$$\beta = (145)\,(298)\,(376)\,.$$

We then see that

$$\beta^k = (145)^k\,(298)^k\,(376)^k = \begin{cases} e & k \text{ is a multiple of 3;} \\ \beta & k-1 \text{ is a multiple of 3;} \\ \beta^2 & k-2 \text{ is a multiple of 3.} \end{cases}$$

as disjoint cycles commute. Hence

$$\beta^{272} = \beta^2 = (154)\,(289)\,(367)\,.$$

■

Notation 66 ***Suppressing 1-cycles.*** *It is typical to not bother writing 1-cycles (or fixed points) of permutations. So – for α, α^{-1} as in the previous example – we will write*

$$\alpha = (1539)\,(26)\,(47) \qquad \textit{and} \qquad \alpha^{-1} = (1935)\,(26)\,(47)$$

with it being understood that 8 is not moved (or more generally any unmentioned elements).

Proposition 67 *Let $\sigma = \rho_1 \cdots \rho_k$ be an expression for σ as disjoint cycles of lengths $l_1, \ldots, l_k$. Then the order of σ equals*

$$\mathrm{lcm}(l_1, \ldots l_k)$$

where lcm *denotes the lowest common multiple. (Given finitely many positive integers, their* ***least common multiple*** *is the smallest positive integer which is a multiple of each of them.)*

Example 68 *(i) How many* 5*-cycles are there in* S_{11}*?*
(ii) How many permutations in S_8 *have a cycle decomposition type of two* 3*-cycles and one* 2*-cycle?*

Solution. (i) 5-cycles in S_{11} are of the form $(a\,b\,c\,d\,e)$. There are 11 choices for what a might be, 10 for b, 9 for c, 8 for d and 7 for e. However we need to remember that

$$(a\,b\,c\,d\,e) = (b\,c\,d\,e\,a) = (c\,d\,e\,a\,b) = (d\,e\,a\,b\,c) = (e\,a\,b\,c\,d)$$

and so there answer is

$$\frac{11 \times 10 \times 9 \times 8 \times 7}{5} = 11088.$$

(ii) Permutations in S_8 that decompose to two 3-cycles and a 2-cycles are of the form

$$(a\,b\,c)\,(d\,e\,f)\,(g\,h)\,.$$

There are 8! ways of filling in these brackets as $a \ldots h$ but we need to remember that the above permutation also equals

$$(b\,c\,a)\,(d\,e\,f)\,(g\,h) = (a\,b\,c)\,(e\,f\,d)\,(g\,h) = (a\,b\,c)\,(d\,e\,f)\,(h\,g) = (d\,e\,f)\,(a\,b\,c)\,(g\,h)\,.$$

The first three are equivalent rewritings that come from cycling elements within cycles whilst the last one comes from permuting two equal length cycles. Hence the number of such permutations is

$$\frac{8!}{3 \times 3 \times 2! \times 2} = \frac{40320}{36} = 1120.$$

(i') Note that we could have tackled the 5-cycle question in this manner as well. Thinking of 5-cycles in S_{11} as having cycle type

$$(a\,b\,c\,d\,e)\,(f)\,(g)\,(h)\,(i)\,(j)\,(k)$$

we see that there are 11! ways of filling these brackets as $a \ldots k$ but 5 ways of cycling $a \ldots e$ and 6! ways of permuting the equal length cycles $(f) \ldots (k)$ Hence the answer is

$$\frac{11!}{5 \times 6!} = 11088.$$

■

Proposition 69 *In* S_n *there are*

$$\frac{n!}{\left(l_1^{k_1} \times l_2^{k_2} \times \cdots \times l_r^{k_r}\right)(k_1! \times k_2! \times \cdots \times k_r!)}$$

permutations with a cycle type of k_1 *cycles of length* l_1*,* k_2 *cycles of length* $l_2, \ldots, k_r$ *cycles of length* l_r*. This decomposition includes* 1*-cycles so that*

$$k_1 l_1 + k_2 l_2 + \cdots + k_r l_r = n.$$

Proof. Put in a fixed order the $\sum k_i$ brackets. As already argued in specific cases, there are $n!$ ways of filling the brackets with the numbers $1, \ldots, n$. However the same permutation can be written as a product of disjoint cycles in many ways as specified in Theorem 63 (though essentially these all being the same). From that theorem we know that there are l_i ways of cycling the elements of each cycle of length l_i and we have $k_i!$ of permuting the cycles of length l_i. Hence $n!$ is an overcount by a factor of

$$\left(l_1^{k_1} \times l_2^{k_2} \times \cdots \times l_r^{k_r}\right)(k_1! \times k_2! \times \cdots \times k_r!)\,.$$

■

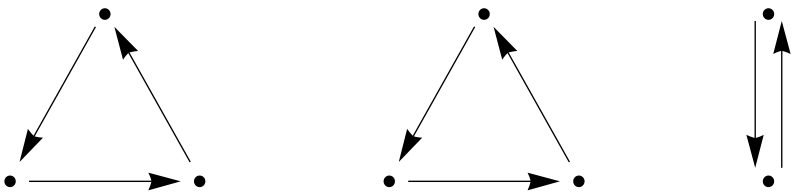
Example 70 *How many permutations of each cycle type are there in S_7?*

Solution. The table below contains the various numbers. We need to consider the various ways in which 7 can be composed as other integers.

type	working	#	type	working	#	type	working	#
7	$7!/7$	720	$4+2$	$7!/(4\times 2)$	630	3	$\frac{7\times6\times5}{3}$	70
6	$7!/6$	840	4	$\frac{7\times6\times5\times4}{4}$	210	3×2	$\frac{7\times6\times5\times4\times3\times2}{2\times2\times2\times3!}$	105
$5+2$	$7!/(5\times 2)$	504	2×3	$\frac{7\times6\times5\times4\times3\times2}{3\times3\times2!}$	280	2×2	$\frac{7\times6\times5\times4}{2\times2\times2!}$	105
5	$\frac{7\times6\times5\times4\times3}{5}$	504	$3+2\times 2$	$\frac{7!}{3\times2\times2\times2!}$	210	2	$\frac{7\times6}{2}$	21
$4+3$	$7!/(4\times 3)$	420	$3+2$	$\frac{7\times6\times5\times4\times3}{3\times2}$	420	e		1

■

Without the labels $1, 2, \ldots, n$ two permutations of the same cycle type would be indistinguishable. For example, a permutation in S_8 which consists of two 3-cycles and one 2-cycle would simply look like



if we were ignorant of which of the eight objects were $1, 2, \ldots, 8$. Here each arrow represents the effect of applying the permutation once. This idea can be more formally captured by the idea of *conjugates.*

Definition 71 *Two permutations $\sigma, \tau \in S_n$ are said to be* ***conjugate*** *in S_n if there exists $\rho \in S_n$ such that*

$$\sigma = \rho^{-1}\tau\rho.$$

Theorem 72 *Two permutations $\sigma, \tau \in S_n$ are conjugate if and only if they have the same cycle type. (i.e. for any given length, the two permutations have the same number of cycles of that length.)*

We first note the following:

Lemma 73 *For any cycle* $(a_1\, a_2\, \ldots\, a_k)$ *and any* $\rho \in S_n$ *we have*

$$\rho^{-1}(a_1\, a_2\, \ldots\, a_k)\rho = (a_1\rho\, a_2\rho\, \ldots\, a_k\rho).$$

Proof. (Of Lemma) This is left to Exercise Sheet 2, Question 3. ■

Proof. (Of Theorem.) Suppose that $\tau = \rho^{-1}\sigma\rho$ and that $\sigma = \psi_1\psi_2 \ldots \psi_r$ where the ψ_i are disjoint cycles. Then

$$\tau = \rho^{-1}\left(\psi_1\psi_2 \ldots \psi_r\right)\rho = \left(\rho^{-1}\psi_1\rho\right)\left(\rho^{-1}\psi_2\rho\right)\cdots\left(\rho^{-1}\psi_r\rho\right)$$

and we see by the previous lemma that the $\rho^{-1}\psi_i\rho$ are disjoint cycles of the same lengths as the ψ_i. Conversely, suppose that σ and τ have the same cycle decomposition type. Then we may line up the cycles in σ and τ of corresponding lengths as

$$\begin{array}{ccccccc} \sigma & = & (a_1\, a_2\, \ldots\, a_k) & (b_1\, b_2\, \ldots\, b_l) & (c_1\, c_2\, \ldots\, c_m) & \cdots \\ & & \downarrow\rho & \downarrow\rho & \downarrow\rho & \downarrow\rho \\ \tau & = & (\alpha_1\, \alpha_2\, \ldots\, \alpha_k) & (\beta_1\, \beta_2\, \ldots\, \beta_l) & (\gamma_1\, \gamma_2\, \ldots\, \gamma_m) & \cdots \end{array}$$

and we define ρ by $a_i\rho = \alpha_i$, $b_i\rho = \beta_i$, $c_i\rho = \gamma_i$, etc. We then have

$$\begin{aligned} \alpha_i\left(\rho^{-1}\sigma\rho\right) &= a_i\sigma\rho = a_{i+1}\rho = \alpha_{i+1} = \alpha_i\tau \quad \text{for} \quad 1 \leqslant i < k \\ \alpha_k\left(\rho^{-1}\sigma\rho\right) &= a_k\sigma\rho = a_1\rho = \alpha_1 = \alpha_k\tau \end{aligned}$$

and similarly for the other cycles. ■

Example 74 *Let*

$$\sigma = (12)\,(34)\,(567)\,, \qquad \tau = (28)\,(17)\,(345)$$

be permutations in S_8.

(i) How many ρ *are there in* S_8 *such that* $\sigma = \rho^{-1}\tau\rho$*?*

(ii) How many $\rho \in S_8$ *are there which commutes with* σ*?*

Solution. (i) We need ρ such that

$$\rho^{-1}\tau\rho = (2\rho\, 8\rho)\,(1\rho\, 7\rho)\,(3\rho\, 4\rho\, 5\rho) = (12)\,(34)\,(567)\,.$$

Thinking about the different ways of rewriting (12) (34) (567) (as the same permutation) we see that we need

$$(2\rho\, 8\rho)\,(1\rho\, 7\rho) = (12)\,(34) \quad \text{and} \quad (3\rho\, 4\rho\, 5\rho) = (567)\,.$$

and so

$$3\rho\ = 5 \text{ or } 6 \text{ or } 7, \qquad 2\rho = 1 \text{ or } 2 \text{ or } 3 \text{ or } 4, \qquad 6\rho = 8.$$

Once we know 3ρ then 4ρ and 5ρ are known (e.g. $3\rho = 6$ implies $4\rho = 7$ and $5\rho = 5$). Once we know 2ρ then we know 8ρ but we still have two choices for 1ρ. In all then we see that there are

$$\underbrace{3}_{\text{choosing } 3\rho} \times \underbrace{4}_{\text{choosing } 2\rho} \times \underbrace{2}_{\text{choosing } 1\rho} = 24$$

such ρ.

(ii) If we replace τ with σ we can still make the same argument to realize that there are 24 such ρ that $\sigma = \rho^{-1}\sigma\rho$. However this is an equivalent equation to $\rho\sigma = \sigma\rho$ so these same 24 permutations commute with σ. ■

Remark 75 *If further asked which these* 24 *permutations are recall that we need*

$$(1\rho\, 2\rho)\,(3\rho\, 4\rho)\,(5\rho\, 6\rho\, 7\rho) = (12)\,(34)\,(567)\,.$$

So the 24 *permutations in fact comprise the group* $D_8 \times C_3$ *where* D_8 *is the symmetry group of the square with labels* $1, 2$ *on one diagonal and* $3, 4$ *on another and* $C_3 = \{e, (567)\,, (576)\}\,.$

Recall now the definition of a *permutation matrix* from Linear Algebra II:

Definition 76 *(i) An* $n \times n$ *matrix is a* ***permutation matrix*** *if each row and each column contain a single entry* 1 *and all other entries are* 0.

(ii) We can associate with $\sigma \in S_n$ *a permutation matrix* P_σ *such that the* 1 *entry in row* i *of* P_σ *is in column* $i\sigma$.

Note that the (i, j)*th entry of* P_σ *is* $\delta_{i\sigma\, j}$.

Example 77 *With* $n = 3$:

$$P_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad P_{(123)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \qquad P_{(132)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Note that $P_{(12)}$ *is self-inverse and that* $P_{(123)}$ *is the inverse of* $P_{(132)}$.

Proposition 78 *(a) For* $\sigma \in S_n$ *then* P_σ *is indeed a permutation matrix.*

(b) For $\sigma, \tau \in S_n$ *then* $P_{\sigma\tau} = P_\sigma P_\tau$.

Proof. (a) By definition P_σ has precisely a single entry 1 in each row. And the only row with an entry of 1 in the ith column is row $i\sigma^{-1}$.

(b) By definition of matrix multiplication

$$(P_\sigma P_\tau)_{ij} = \sum_{k=1}^{n} (P_\sigma)_{ik}\,(P_\tau)_{kj} = \sum_{k=1}^{n} \delta_{i\sigma\, k}\,\delta_{k\tau\, j} = \delta_{i\sigma\tau\, j} = (P_{\sigma\tau})_{ij}\,.$$

■

We will make use of permutation matrices in showing that the *parity* of a permutation is well-defined.

Definition 79 *(i) A* ***transposition*** *is another term for a* 2*-cycle.*

(ii) A permutation is said to be **odd** *(resp.* **even**) *if it can be written as a product of an odd (resp. even) number of transpositions.*

Lemma 80 *If* σ *is a transposition then* $\det P_\sigma = -1$.

Proof. This is equivalent to knowing that swapping two rows of a matrix multiplies its determinant by -1. For if $\sigma = (ij)$ then

$$\det P_\sigma = \det\left(I_n \text{ with rows } i \text{ and } j \text{ swapped}\right) = -\det I_n = 1.$$

■

Theorem 81 *(a) Every permutation can be written as a product of transpositions (and consequently is either even and/or odd).*

(b) No permutation is both even and odd.

Proof. (a) Any permutation my be written as a product of disjoint cycles by Theorem 63. And any cycle may be written as a product of transpositions as

$$(a_1\, a_2\, a_3 \cdots a_k) = (a_1 a_2)\,(a_1 a_3) \cdots (a_1 a_k)$$

as the product of transpositions has the effect

$$a_1 \underbrace{\to}_{(a_1 a_2)} a_2 \underbrace{\to}_{\text{remainder}} a_2, \qquad a_i \underbrace{\to}_{\text{first } i-2} a_i \underbrace{\to}_{(a_1 a_i)} a_1 \underbrace{\to}_{(a_1 a_{i+1})} a_{i+1} \underbrace{\to}_{\text{remainder}} a_{i+1} \text{ for } i \geqslant 2.$$

(b) If σ is expressible as the product of k transpositions, then by the above lemma $\det P_\sigma = (-1)^k$. Hence no permutation can be both even and odd. ■

Remark 82 *Note that cycles of even (resp. odd) length are (somewhat annoyingly) odd (resp. even). So a permutation is even if and only if its cycle type has an even number of even length cycles.*

Example 83 *If we return to Example 70 then we see that the following permutations were the even ones.*

type	*working*	#	*type*	*working*	#	*type*	*working*	#
7	$7!/7$	720	2×3	$\frac{7\times6\times5\times4\times3\times2}{3\times3\times2!}$	280	2×2	$\frac{7\times6\times5\times4}{2\times2\times2!}$	105
5	$\frac{7\times6\times5\times4\times3}{5}$	504	$3 + 2 \times 2$	$\frac{7!}{3\times2\times2\times2!}$	210	e		1
$4 + 2$	$7!/\left(4 \times 2\right)$	630	3	$\frac{7\times6\times5}{3}$	70		*TOTAL*	2520

Note that precisely half the permutations are even.

Proposition 84 *(a) The even permutations in S_n form a subgroup A_n.*
(b) For $n \geqslant 2$, the order of A_n is $\frac{1}{2}n!$.
(c) A_n is non-abelian for $n \geqslant 4$.
A_n is called the ***alternating group****.*

Proof. (a) If

$$\sigma = \rho_1 \rho_2 \cdots \rho_{2k} \qquad \text{and} \qquad \tau = \psi_1 \psi_2 \cdots \psi_{2l}$$

are expressions for σ and τ as products of even numbers of transpositions then

$$\sigma\tau = \rho_1 \rho_2 \cdots \rho_{2k} \psi_1 \psi_2 \cdots \psi_{2l} \qquad \text{and} \qquad \sigma^{-1} = \rho_{2k} \rho_{2k-1} \cdots \rho_1$$

are clearly even. The identity is also even as e is the product of zero transpositions. Hence A_n is a subgroup of S_n.

(b) The permutation (12) is odd; so the maps

$$A_n \to A_n^c \text{ given by } \sigma \mapsto (12)\sigma; \qquad A_n^c \to A_n \text{ given by } \sigma \mapsto (12)\sigma;$$

are inverses of one another and so $|A_n| = |A_n^c| = \frac{1}{2}n!$.

(c) If $n \geqslant 4$ then note (123) and (124) are even permutations which do not commute. ■

Example 85 (123) *and* (132) *are not conjugate in* A_4.

Solution. Suppose that $\sigma^{-1}(123)\sigma = (132)$. Then $(1\sigma\, 2\sigma\, 3\sigma) = (132)$. As

$$(132) = (213) = (321)$$

are the only ways to write the permutation (132) then there are three possibilities

$$\begin{aligned} 1\sigma &= 1, \quad 2\sigma = 3, \quad 3\sigma = 2, \quad 4\sigma = 4; \\ 1\sigma &= 2, \quad 2\sigma = 1, \quad 3\sigma = 3, \quad 4\sigma = 4; \\ 1\sigma &= 3, \quad 2\sigma = 2, \quad 3\sigma = 1, \quad 4\sigma = 4. \end{aligned}$$

That is σ equals (23) or (12) or (13). As none of these is even, then (123) and (132) are not conjugate in A_4. ■

Example 86 *The conjugacy classes in* A_4 *are* $\{e\}$ *and*

$$\{(12)(34), (13)(24), (14)(23)\}, \quad \{(123), (134), (214), (324)\}, \quad \{(132), (143), (124), (234)\}.$$

Solution. Note that

$$(123)^{-1}(12)(34)(123) = (23)(14), \qquad (123)^{-1}(23)(14)(123) = (31)(24).$$

Also

$$(123)^{-1}(134)(123) = (214), \quad (123)^{-1}(214)(123) = (324), \quad (134)^{-1}(214)(134) = (123).$$

As conjugacy in A_4 implies conjugacy in S_4 (though not conversely) and a 3-cycle is not conjugate in A_4 with its inverse (by the previous example), then the conjugacy classes in A_4 are as given. ■

3. MORE ON SUBGROUPS & CYCLIC GROUPS

Recall that we say a subset H of a group G is a **subgroup of** G if H is a group in its own right under the restriction of G's group operation. We write this

$$H \leqslant G.$$

There is a simple check – the *subgroup test* – for determining whether a subset is a subgroup.

Proposition 87 *(**Subgroup Test**) Let G be a group. Then $H \subseteq G$ is a subgroup of G if and only if H is non-empty and whenever $x, y \in H$ then $x^{-1}y \in H$.*

Proof. $\Longrightarrow$ Suppose that $H \leqslant G$. Then $e \in H$ and so H is non-empty. Further for $x, y \in H$ we have $x^{-1}y \in H$ as H is closed under products and inverses.

$\Longleftarrow$ Suppose that the subgroup test applies. As $H \neq \varnothing$ then there is some $h \in H$ and so by the test $e = h^{-1}h \in H$. Further if $x, y \in H$ then by the test $x^{-1} = x^{-1}e \in H$ and $xy = (x^{-1})^{-1}y \in H$. Thus H is closed under products and inverses. Finally the associativity of the group operation on H is inherited from its associativity on G. ■

Example 88 *The subgroups of S_3 are*

$$\{e\}, \qquad \{e,(12)\}, \qquad \{e,(13)\}, \qquad \{e,(23)\}, \qquad A_3, \qquad S_3.$$

Solution. The listed subgroups are certainly subgroups of S_3. To see that these are the only subgroups suppose that $H \leqslant S_3$. Certainly $e \in H$. If $|H| = 2$ then H must consist of e and a non-trivial self-inverse element. If $|H| = 3$ then it must be of the form $\{e, g, g^2\}$ where $g^3 = e$ and A_3 is the only such subgroup. If $|H| \geqslant 4$ then H must either (i) contain all three 2-cycles or (ii) a 2-cycle and a 3-cycle. As the product of two 2-cycles in S_3 is a 3-cycle, we see case (ii) in fact subsumes case (i). Also if H contains a 3-cycle then it contains its inverse. So, without any loss of generality we may assume this 2-cycle and 3-cycle to be (12) and (123). But then

$$(13) = (12)(123), \qquad (23) = (123)(12), \qquad (132) = (123)^2$$

and we see that $H = S_3$. ■

Example 89 *The subgroups of D_8 are*

$$\begin{gathered}\{e\}, \qquad \{e,r^2\}, \qquad \{e,s\}, \qquad \{e,rs\}, \qquad \{e,r^2s\}, \qquad \{e,r^3s\}, \\ \{e,r,r^2,r^3\}, \qquad \{e,r^2,s,r^2s\}, \qquad \{e,r^2,rs,r^3s\}, \qquad D_8.\end{gathered}$$

Solution. The listed subgroups are certainly subgroups of D_8. To see that these are the only subgroups suppose that $H \leqslant D_8$. Certainly $e \in H$. If $|H| = 2$ then H must consist of e and a non-trivial self-inverse element and the possibilities are listed above. If $|H| = 3$ then it must be of the form $\{e, g, g^2\}$ where $g^3 = e$ but there is no such $g \in D_8$. A subgroup of order 4 must be of the form $\{e,g,g^2,g^3\}$ where $g^4=e$ or $\{e,a,b,ab\}$ where $a^2=b^2=e$ and $ab=ba$. For the former, only $g=r$ or $g=r^3$ will do which both lead to the same subgroup $\{e,r,r^2,r^3\}$. For the latter we must have two reflections and a rotation; further the rotation must be r^2 if it is to commute with the reflections. So the only possibilities are $\{e,r^2,s,r^2s\}$ and $\{e,r^2,rs,r^3s\}$. If $|H|\geqslant 5$ then H must contain a rotation and a reflection; if the rotation is r or r^3 then it and the reflection will lead to all of D_8 but if there are three or more reflections then at least one must be in a diagonal and one in the vertical or horizontal and so their product is r or r^3. Hence $H=D_8$ is the only subgroup of order greater than 4. ■

Example 90 *The subgroups of $C_6=\{e,g,g^2,g^3,g^4,g^5\}$ are*

$$\{e\},\qquad \{e,g^3\},\qquad \{e,g^2,g^4\},\qquad C_6.$$

The only subgroups of C_5 are $\{e\}$ and C_5.

Solution. The only non-trivial self-inverse element in C_6 is g^3 and the non-trivial solutions of $x^3=e$ are g^2,g^4. If $H\leqslant C_6$ and $|H|\geqslant 4$ then either $g\in H$ or $g^5=g^{-1}\in H$ (both of which lead to $H=C_6$) or $\{e,g^2,g^3,g^4\}\subseteq H$ in which case $g^3\left(g^2\right)^{-1}=g\in H$ in which case $H=C_6$ is the same conclusion.

If $H\leqslant C_5$ and $g\in H$ then $H=C_5$ but if $g^2\in H$ then $\left(g^2\right)^3=g\in H$, and if $g^3\in H$ then $\left(g^3\right)^{-1}=g^2\in H$ and if $g^4\in H$ then $\left(g^4\right)^{-1}=g\in H$. So $H=\{e\}$ or $H=C_5$. ■

Remark 91 *You may have noticed that in each of the previous examples, $|H|$ divides $|G|$ and this is indeed the case. This result is known as* ***Lagrange's Theorem*** *which we will prove in the next chapter.*

Proposition 92 *Let G be a group and H,K be subgroups of G. Then $H\cap K$ is a subgroup.*

Proof. This is left as Exercise Sheet 3, Question 2. ■

In fact, it is very easy to generalize Proposition 92 to show that if H_i (where $i\in I$) form a collection of subgroups of G then

$$\bigcap_{i\in I}H_i\leqslant G.$$

Thus we may make the following definition.

Definition 93 *Let G be a group and S a subset of G.*
(i) The ***subgroup generated by*** *S, written $\langle S\rangle$, is the smallest subgroup of G which contains S. (This is well-defined as G is a subgroup of G which contains S and $\langle S\rangle$ is then the intersection of all such subgroups.)*
(ii) If $g\in G$, then we write $\langle g\rangle$ rather than the more accurate but cumbersome $\langle\{g\}\rangle$.
(iii) If $\langle S\rangle=G$ then the elements of S are said to be ***generators*** *of G.*

Example 94 *Determine $\langle S\rangle$ in each of the following cases:*
(i) $G=\mathbb{Z}$, $S=\{12,42\}$.
(ii) $G=S_4$, $S=\{(123),(12)(34)\}$.
(iii) $G=\mathbb{Q}^*$, $S=\{3,\frac{2}{3}\}$.

Solution. (i) Note that $6 = 42 - 3 \times 12$; hence $6 \in \langle S\rangle$ and $6\mathbb{Z} \subseteq \langle S\rangle$. But as $12 = 2 \times 6$ and $42 = 7 \times 6$ then $\langle S\rangle \subseteq 6\mathbb{Z}$. This $\langle S\rangle = 6\mathbb{Z}$.

(ii) As $(123) \in A_4$ and $(12)(34) \in A_4$ then certainly $\langle S\rangle \subseteq A_4$. If we write $\sigma = (123)$ and $\tau = (12)(34)$ then we see that the following are also in A_4.

$$\begin{array}{cccc} e, & \sigma = (123), & \tau\sigma\tau = (214), & (\tau\sigma\tau)^2 = (124)\,, \\ \sigma^2\tau\sigma = (14)(23), & \sigma\tau\sigma^2 = (13)(24), & \tau = (12)(34), & \sigma^2 = (132), \\ \sigma\tau = (243), & (\sigma\tau)^2 = (234), & \tau\sigma = (134), & (\tau\sigma)^2 = (143). \end{array}$$

Hence $\langle S\rangle = A_4$.

(iii) We have $3 \in \langle S\rangle$ and so $3^m \in \langle S\rangle$ for all $m \in \mathbb{Z}$. Likewise $2 = \frac{2}{3} \times 3 \in \langle S\rangle$ so that $2^n \in \langle S\rangle$ for all $n \in \mathbb{Z}$. So $2^n 3^m \in \langle S\rangle$ for $m, n \in \mathbb{Z}$. But as these form a subgroup of $\mathbb{Q}^*$ (see the next example) we have

$$\langle S\rangle = \{2^n 3^m \colon m, n \in \mathbb{Z}\}.$$

■

Example 95 *Show that if G is abelian and $g, h \in G$ then*

$$\langle g, h\rangle = \{g^r h^s \colon r, s \in \mathbb{Z}\}\,.$$

Solution. Certainly $\{g^r h^s \colon r, s \in \mathbb{Z}\} \subseteq \langle g, h\rangle$. However, when G is abelian (or indeed if just $gh = hg$), then $\{g^r h^s \colon r, s \in \mathbb{Z}\}$ is a subgroup as follows:

(i) $e = g^0 h^0 \in \{g^r h^s \colon r, s \in \mathbb{Z}\}\,;$

(ii) $\left(g^k h^l\right)\left(g^K h^L\right) = g^{k+K} h^{l+L} \in \{g^r h^s \colon r, s \in \mathbb{Z}\}\,;$

(iii) $\left(g^k h^l\right)^{-1} = h^{-l} g^{-k} = g^{-k} h^{-l} \in \{g^r h^s \colon r, s \in \mathbb{Z}\}\,.$ ■

Remark 96 *In several of the results that follow, notably Proposition 97 and Theorem 102 we make use of the following fact, known as the* ***division algorithm****, which we will take as self-evident.*

- *Let a, b be integers with $b > 0$. Then there exist unique integers q, r such that $a = qb + r$ and $0 \leqslant r < b$.*

Proposition 97 *Let G be a group and $g \in G$. Then*

(a) $\langle g\rangle = \left\{g^k \colon k \in \mathbb{Z}\right\}$.

(b) If $\mathrm{o}(g)$ is finite then $\langle g\rangle = \left\{e, g, g^2, \ldots, g^{\mathrm{o}(g)-1}\right\}$.

Proof. (a) As $g^k \in \langle g\rangle$ for any integer k, so it only remains to show that $H = \left\{g^k \colon k \in \mathbb{Z}\right\}$ is indeed a subgroup. Using the subgroup test we note $g^0 = e \in H$ and that if $g^k, g^l \in H$ then

$$(g^k)^{-1} g^l = g^{-k} g^l = g^{l-k} \in H.$$

Hence $\langle g\rangle = H$.

(b) It is again clear that $\left\{e, g, g^2, \ldots, g^{\mathrm{o}(g)-1}\right\} \subseteq \langle g\rangle$. Also for any $k \in \mathbb{Z}$ there exist $q, r \in \mathbb{Z}$ such that $k = q\mathrm{o}(g) + r$ where $0 \leqslant r < \mathrm{o}(g)$. Then

$$g^k = g^{q\mathrm{o}(g)+r} = \left(g^{\mathrm{o}(g)}\right)^q g^r = e^q g^r = g^r \in \left\{e, g, g^2, \ldots, g^{\mathrm{o}(g)-1}\right\}.$$

■

Remark 98 *Recall that we say that a group G is* **cyclic** *if there exists $g \in G$ such that $G = \langle g \rangle$. Note also that a cyclic group is necessarily abelian.*

Remark 99 *Note that in a finite group G, then g is a generator if and only if $\mathrm{o}(g) = |G|$.*

Example 100 *(i) C_6 is cyclic with generators g and g^5.*

(ii) C_5 is cyclic with generators g, g^2, g^3, g^4.

(iii) $C_2 \times C_2$ is not cyclic as the elements have orders $1, 2, 2, 2$.

(iv) $C_2 \times C_3$ is cyclic. If $C_2 = \{e, g\}$ and $C_3 = \{e, h, h^2\}$ then (g, h) and (g, h^2) are both generators of $C_2 \times C_3$ as they have order 6 (check!).

(v) $\mathbb{Q}$ is not cyclic: clearly $\langle 0 \rangle \neq \mathbb{Q}$ and if $q \neq 0$ then $\frac{1}{2}q \notin \langle q \rangle = q\mathbb{Z}$. By the same reasoning we see that $\mathbb{Q}$ cannot be generated by finitely many elements.

Theorem 101 *Let G be a cyclic group.*

(a) If $|G| = n$ is finite, then G is isomorphic to C_n.

(b) If $|G|$ is infinite, then G is isomorphic to $\mathbb{Z}$.

Proof. (a) Let g be a generator of G. Then

$$G = \langle g \rangle = \left\{e, g, g^2, \ldots, g^{n-1}\right\}$$

by Proposition 97 (b) and multiplication in G is as given in Example 34 as $g^n = e$.

(b) If g is a generator of G with infinite order, then we can define a map $\phi \colon G \to \mathbb{Z}$ by $\phi(g^r) = r$ which is an isomorphism. ■

Theorem 102 *Let G be a cyclic group and $H \leqslant G$. Then H is cyclic.*

Proof. Let $G = \langle g \rangle$. If $H = \{e\}$ then $H = \langle e \rangle$ and we are done. Otherwise, we define

$$n = \min\left\{k > 0 \colon g^k \in H\right\}.$$

To show that n is well-defined, note that $g^k \in H \neq \{e\}$ for some $k \neq 0$. As H is a subgroup then $g^{-k} = \left(g^k\right)^{-1} \in H$ also. As one of $\pm k$ is positive, n is well-defined. We will show that

$$H = \langle g^n \rangle.$$

As $g^n \in H$ then $\langle g^n \rangle \subseteq H$. Conversely say that $g^a \in H$. Then, by the division algorithm, there exist $q, r \in \mathbb{Z}$ such that $a = qn + r$ where $0 \leqslant r < n$. But then

$$g^r = g^{a-qn} = g^a \left(g^n\right)^{-q} \in H$$

as $g^a \in H$ and $g^n \in H$. By the minimality of n then $r = 0$ and $g^a = (g^n)^q \in \langle g^n \rangle$. ■

Corollary 103 *The subgroups of $\mathbb{Z}$ are each of the form $m\mathbb{Z}$ where $m \in \mathbb{Z}$.*

Proposition 104 *Let m, n be non-zero integers. By Theorem 102 we have*

$$\langle m, n\rangle = \langle h\rangle \qquad \langle m\rangle \cap \langle n\rangle = \langle l\rangle$$

for some $h, l > 0$. Then h has the following properties:
(a) $h|m$ and $h|n$;
(b) if $x|m$ and $x|n$ then $x|h$;
(c) there exist $u, v \in \mathbb{Z}$ such that $um + vn = h$. ***(Bézout's Lemma)***
and l has the following properties:
(d) $m|l$ and $n|l$;
(e) if $m|x$ and $n|x$ then $l|x$.

Proof. Properties of h:
(a) As $m = 1m + 0n \in \langle m, n\rangle = \langle h\rangle$ then $h|m$. Similarly $h|n$.
(c) This follows from Example 95.
(b) Say $x|m$ and $x|n$. Then by Bézout's Lemma $x|um + vn$ and so $x|h$.
Properties of l:
(d) As $l \in \langle m\rangle$ then $m|l$. Similarly $n|l$.
(e) If $m|x$ then $x \in \langle m\rangle$. Likewise $x \in \langle n\rangle$. So $x \in \langle m\rangle \cap \langle n\rangle = \langle l\rangle$ and $l|x$. ■

Definition 105 *We define h, as defined in the previous Proposition, to be the* ***highest common factor*** *or* ***hcf*** *of m and n.*

We define l as defined in the previous Proposition, to be the ***least common multiple*** *or* ***lcm*** *of m and n.*

Theorem 106 ***(Chinese Remainder Theorem)*** *Let m and n be coprime natural numbers. Then C_{mn} is isomorphic to $C_m \times C_n$.*

Specifically if g is a generator of C_m and h is a generator of C_n then (g, h)generates $C_m \times C_n$.

Proof. Certainly

$$(g, h)^{mn} = ((g^m)^n, (h^n)^m) = (e^n, e^m) = (e, e)$$

so that the order of (g, h) divides mn. But on the other hand $g^k = e$ if and only if $m|k$ and $h^k = e$ if and only if $n|k$. So

$$(g, h)^k = \left(g^k, h^k\right) = (e, e)$$

if and only if $m|k$ and $n|k$. As m, n are coprime then, by Bezout's Lemma, there exist u, v such that $um + vn = 1$. As $n|k$ then $mn|mk$ and as $m|k$ then $mn|nk$. So

$$mn \mid (umk + vnk) = k.$$

Hence the order of (g, h) is mn which equals $|C_m \times C_n|$. ■

4. REPRISE ON EQUIVALENCE RELATIONS

Firstly we recall:

Definition 107 *A (binary)* ***relation*** $\sim$ *on a set* S *is a subset of* $S \times S$*.*

$$\textit{Then, for } a, b, \in S, \textit{ we write } a \sim b \textit{ if and only if } (a,b) \in \sim .$$

We might just as easily view the relation as a function $\sim : S \times S \to \{T, F\}$*, that is a function with two inputs from* S *and output True* (T) *or False* (F)*. The "set"* $\sim$ *would then be* $\sim^{-1}(T)$*.*

Example 108 *(i) With* $S = \mathbb{Z}$*, we would have "*$\leqslant (3,4) = T$*" or "*$(3,4) \in \leqslant$*" as rather unnatural ways of simply saying "*$3 \leqslant 4$*".*
(ii) If $S = \{1,2,3\}$ *then* $<$ *is the set* $\{(1,2),\ (1,3),\ (2,3)\}$*.*

Definition 109 *We say that a relation* $\sim$ *on a set* S *is an equivalence relation if it is*
(i) ***reflexive*** *– that is* $a \sim a$ *for all* $a \in S$*;*
(ii) ***symmetric*** *– that is, whenever* $a \sim b$ *then* $b \sim a$*;*
(iii) ***transitive*** *– that is, whenever* $a \sim b$ *and* $b \sim c$ *then* $a \sim c$*.*

Example 110 *The following are all examples of equivalence relations:*
(i) $S = \mathbb{C}$ *with* $z \sim w$ *iff* $|z| = |w|$*;*
(ii) $S = GL(n, \mathbb{R})$ *with* $A \sim B$ *iff there exists* $P \in GL(n, \mathbb{R})$ *such that* $A = P^{-1}AP$;
(iii) $S = \{\textit{polygons in } \mathbb{R}^2\}$ *and* $\sim$ *is congruence;*
(iv) $S = \mathcal{P}(X)$ *and* $A \sim B$ *if* $|A| = |B|$*;*
(v) S *is a group and* $x \sim y$ *if* $x = y$ *or* $x = y^{-1}$*;*
(vi) $S = C^1(\mathbb{R})$ *with* $f(x) \sim g(x)$ *if* $f'(x) = g'(x)$*.*

Example 111 *The following relations* ***aren't*** *equivalence relations:*
(i) $S = \mathbb{Z}$ *with* $m \sim n$ *iff* $m < n$ *as* $\sim$ *isn't reflexive or symmetric;*
(ii) $S = \mathcal{P}(X)$ *with* $A \sim B$ *iff* $A \subseteq B$ *as* $\sim$ *isn't symmetric;*
(iii) $S = \mathbb{R}[x]$ *with* $p(x) \sim q(x)$ *iff* $p(a) = q(a)$ *for some* $a \in \mathbb{R}$ *as* $\sim$ *isn't transitive.*

Proposition 112 *Let* $S = \mathbb{Z}$ *and* $n \geqslant 2$ *is an integer. If we set* $a \sim b$ *if* $a - b$ *is a multiple of* n *then* $\sim$ *is an equivalence relation.*

Proof. (a) For any $a \in \mathbb{Z}$ we have $a \sim a$ as 0 is a multiple of n.
(b) If $a \sim b$ then $a - b = kn$ for some integer k. Then $b - a = -kn$ and hence $b \sim a$.
(c) If $a \sim b$ and $b \sim c$ then $a - b = kn$ and $b - c = ln$ for integers k, l. But then

$$a - c = (a - b) + (b - c) = (k + l)n$$

and hence $a \sim c$. ■

Definition 113 *Let G be a group and $g, h \in G$. Then g and h are said to be* ***conjugate in*** G *if there exists $k \in G$ such that $g = k^{-1}hk$. (Compare with Definition 71.)*

Proposition 114 *Conjugacy is an equivalence relation.*

Proof. Let G be a group and write $g \sim h$ if there exists k such that $g = k^{-1}hk$. Then:
(a) $\sim$ is reflexive as $g = e^{-1}ge$ for all g.
(b) If $g = k^{-1}hk$ then $h = kgk^{-1} = \left(k^{-1}\right)^{-1} gk^{-1}$ and hence $\sim$ is symmetric.
(c) If $g_1 \sim g_2$ and $g_2 \sim g_3$ then there exist k_1 and k_2 such that

$$g_1 = k_1^{-1} g_2 k_1 \qquad \text{and} \qquad g_2 = k_2^{-1} g_3 k_2.$$

Hence $g_1 = k_1^{-1} k_2^{-1} g_3 k_2 k_1 = \left(k_2 k_1\right)^{-1} g_3 \left(k_2 k_1\right)$. ■

Definition 115 *Given an equivalence relation $\sim$ on a set S with $a \in S$, then the* ***equivalence class of*** a*, written $\bar{a}$ or $[a]$, is the set*

$$\bar{a} = \{x \in S \colon x \sim a\}.$$

Example 116 *Given the equivalence relation in Proposition 112 there are n equivalence classes namely $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$. This follows from the division algorithm in $\mathbb{Z}$. We see that*

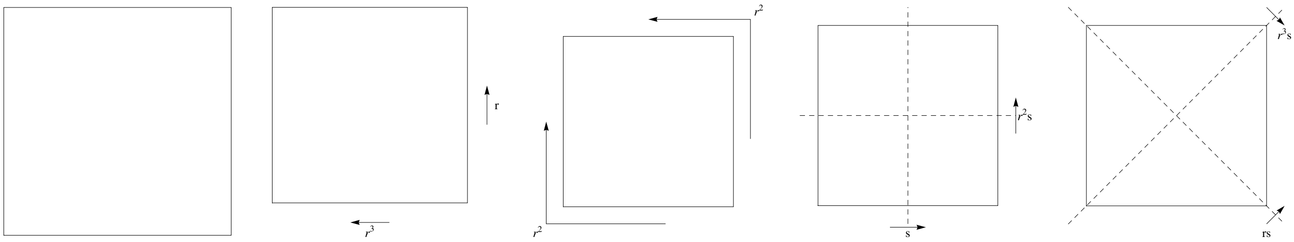
$$\bar{0} = n\mathbb{Z}; \qquad \bar{1} = 1 + n\mathbb{Z}; \qquad \ldots \qquad \overline{n-1} = (n-1) + n\mathbb{Z} = -1 + n\mathbb{Z}.$$

Example 117 *The conjugacy class of σ in S_n are those permutations of the same cycle type.*

Example 118 *The conjugacy classes of D_8 are*

$$\{e\}, \quad \left\{r, r^3\right\}, \quad \left\{r^2\right\}, \quad \left\{s, r^2 s\right\}, \quad \left\{rs, r^3 s\right\}.$$

Diagrammatically it is a little clearer as to what is going on

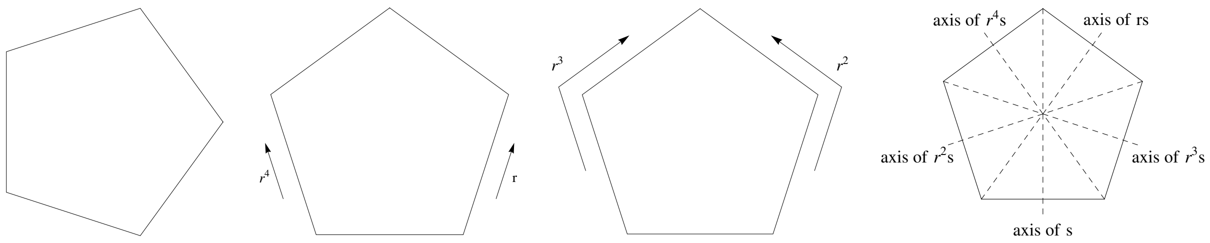


Depending on their viewpoints, two observers might confuse reflection in the horizontal with it in the vertical, but will be certain that the square wasn't reflected in a diagonal; likewise they might conflate rotation by a right angle anticlockwise with the same in a clockwise fashion.

For D_{10} the conjugacy classes are

$$\{e\}, \quad \left\{r, r^4\right\}, \quad \left\{r^2, r^3\right\}, \quad \left\{s, rs, r^2 s, r^3 s, r^4 s\right\}.$$

Again, diagrammatically, it is a little clearer as to what is going on



The general cases are investigated in Exercise Sheet 5, Question 3.

Definition 119 *Let S be a set and Λ be an indexing set. We say that a collection of subsets A_λ of S (where $\lambda \in \Lambda$) is a partition of S if*

(i) $A_\lambda \neq \varnothing$ for each $\lambda \in \Lambda$;

(ii) $\bigcup\limits_{\lambda \in \Lambda} A_\lambda = S$;

(iii) if $\lambda \neq \mu$ then $A_\lambda \cap A_\mu = \varnothing$, or equivalently: if $A_\lambda \cap A_\mu \neq \varnothing$ then $\lambda = \mu$.

Notation 120 *Given a partition P of S and $a \in S$, we will write P_a for the unique set in P such that $a \in P_a$.*

Theorem 121 *Let $\sim$ be an equivalence relation on a set S. Then the $\sim$-equivalence classes partition S.*

Proof. Firstly, $a \in \bar{a}$ for any $a \in S$ by reflexivity; this shows that equivalence classes are non-empty and also that their union is S. Secondly, we need to show that distinct equivalence classes are disjoint. So suppose that $c \in \bar{a} \cap \bar{b}$ for $a, b, c \in S$. We need to show that $\bar{a} = \bar{b}$. As $c \in \bar{a}$ then $c \sim a$ and likewise $c \sim b$. By symmetry and transitivity it follows that $a \sim b$. So if $x \in \bar{a}$ we have $x \sim a \sim b$ and hence, by transitivity, $x \sim b$. We have shown that $\bar{a} \subseteq \bar{b}$. If we swap the roles of a and b in the above argument then $\bar{b} \subseteq \bar{a}$ and the result follows. ■

Theorem 122 *Let S be a set.*

(a) Given an equivalence relation $\sim$ on S then the equivalence classes of $\sim$ form a partition $P(\sim)$ of S (where $P(\sim)_a = \bar{a}$ for each $a \in S$).

(b) Given a partition P of S then the relation $\sim_P$ on S defined by

$$a \sim_P b \textit{ if and only if } b \in P_a$$

is an equivalence relation on S.

(c) As given above, (a) and (b) are inverses of one another; that is

$$P(\sim_P) = P \qquad \textit{and} \qquad \sim_{P(\sim)} = \sim .$$

In particular, there are as many equivalence relations on a set S as there are partitions of the set S.

Proof. (a) was proven in the previous theorem. To prove (b), suppose that P is a partition of S.

- Let $a \in S$. Then $a \in P_a$ by definition and so $a \sim_P a$.

- If $a \sim_P b$ then $b \in P_a$ and $b \in P_b$ by definition. So $b \in P_a \cap P_b \neq \varnothing$ and hence $P_a = P_b$. Thus $a \in P_b$ and $b \sim_P a$.

- If $a \sim_P b$ and $b \sim_P c$ then $b \in P_a$ and $c \in P_b$. As $b \in P_a \cap P_b \neq \varnothing$ then $P_a = P_b$ and so $c \in P_a$ and $a \sim_P c$.

(c) Let P be a partition of S.

$$\begin{aligned} A \in P(\sim_P) &\iff \text{there is } a \in A \text{ such that } A \text{ is the } \sim_P\text{-equivalence class of } a \\ &\iff \text{there is } a \in A \text{ such that } A = P_a \\ &\iff A \in P. \end{aligned}$$

Likewise

$$a \sim_{P(\sim)} b \iff b \in (P(\sim))_a \iff a \in \bar{b} \iff a \sim b.$$

■

Example 123 *There are* 52 *equivalence relations on a set with* 5 *elements.*

Solution. Let $X = \{1, 2, 3, 4, 5\}$. As the only ways to partition the integer 5 is

$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$$

and for each such possibility there correspond the following partitions of X

Partition of 5	Partitions of X
5	1
$4+1$	$\binom{5}{1} = 5$
$3+2$	$\binom{5}{2} = 10$
$3+1+1$	$\binom{5}{3} = 10$
$2+2+1$	$\frac{1}{2!}\binom{5}{2}\binom{3}{2} = 15$
$2+1+1+1$	$\binom{5}{2} = 10$
$1+1+1+1+1$	1

■

Example 124 *How many partitions are there of a set with* 22 *elements into* 4 *subsets of size* 3 *and* 2 *subsets of size* 5*?*

Solution. The answer is 1254751898400 counted either of the following ways:

$$\frac{\overbrace{\binom{22}{3}\binom{19}{3}\binom{16}{3}\binom{13}{3}\binom{10}{5}\binom{5}{5}}^{\text{ways of filling the six sets}}}{\underbrace{4!2!}_{\text{shuffling same-size subsets}}} = \frac{\overbrace{22!}^{\text{ways of placing the 22 elements}}}{\underbrace{(3!)^4\,(5!)^2}_{\text{shuffling within subsets}} \times \underbrace{4!2!}_{\text{shuffling same-size subsets}}}.$$

■

4.1 Modular Arithmetic

Consider the odd and even integers. The product of two odd integers is an odd integer, no matter what odd integers we have in mind. Likewise we can see, for example, that

$$\text{Even} \times \text{Odd} = \text{Even}, \qquad \text{Odd} + \text{Odd} = \text{Even},$$

again irrespective of the even and odd numbers we have in mind. If we fill out the addition and multiplication tables for {Even, Odd} then we obtain

+	Even	Odd
Even	Even	Odd
Odd	Odd	Even

,

×	Even	Odd
Even	Even	Even
Odd	Even	Odd

.

You may notice that {Even, Odd} under + makes an abelian group with Even being the additive identity.

More properly the above tables describe the arithmetic of the integers "modulo 2" or more simply "mod 2". **Modular arithmetic** is the study of remainders. If we divide an integer by 2 then there are two possible remainders 0 (when the integer is even) and 1 (when the integer is odd). We could instead rewrite the above addition and multiplication with 0 replacing Even and 1 replacing Odd. The tables would then look like:

+	0	1
0	0	1
1	1	0

,

×	0	1
0	0	0
1	0	1

.

Most of those calculations look fairly natural with the exception of $1 + 1 = 0$, but recall the equation is really conveying that an odd number added to an odd number makes an even number. From the point of view of remainders, adding the two remainders of 1 makes a whole new factor of 2; these two 1s add to *clock* back to 0.

In fact, modular arithmetic is sometimes also referred to as **clockwork arithmetic** and another everyday example of modular arithmetic is the 12-hour clock. It would not be at all surprising for me to say that 5 hours after 9 o'clock comes 2 o'clock or that 7 hours before 1 o'clock was 6 o'clock or that 7 three-hour shifts that started at 2 o'clock will end at 11 o'clock. In mod 12 arithmetic we would write these calculations as

$$5 + 9 = 2, \qquad 1 - 7 = 6, \qquad 2 + 7 \times 3 = 11.$$

These facts are true irrespective of what day of the week we are discussing or whether 5 represents 5am or 5pm.(The only significant difference between $\operatorname{mod} 12$ arithmetic and the 12-hour clock is that we write 0, instead of 12, for noon and midnight.)

More generally, we can use the division algorithm to describe the possible remainders when we divide by any integer $n \geqslant 2$.

Definition 125 *If we are doing arithmetic* $\bmod n$, *(where* $n \geqslant 2$*) then, by the division algorithm, there are* n *possible remainders, namely*

$$0, 1, 2, 3, \ldots, n-1.$$

We define here rules for how to add, subtract and multiply these n *remainders in* $\bmod n$ *arithmetic. Take* $a, b \in \{0, 1, 2, \ldots, n-1\}$. *It may well be the case that* $a+b, a-b$ *or* ab *aren't on this list, but the remainders of this sum, difference and product will be. We may define* $\bmod n$ *addition, subtraction and multiplication by:*

$$\begin{aligned} a+b &= \textit{remainder when } a+b \textit{ is divided by } n; \\ a-b &= \textit{remainder when } a-b \textit{ is divided by } n; \\ ab &= \textit{remainder when } ab \textit{ is divided by } n. \end{aligned}$$

Notation 126 *We write* $\mathbb{Z}_n$ *for the set of remainders* $\{0, 1, 2, \ldots, n-1\}$ *under the operations of* $\bmod n$ *arithmetic. Also we will write* $\bmod n$ *besides a sum, difference or product to denote that we are doing these operations in the context of* $\bmod n$ *arithmetic.*

Example 127 *In* $\bmod 7$ *arithmetic we have*

$$\begin{aligned} 3+6 &= 2 \quad \bmod 7 \textit{ as } 3+6=9 \textit{ and } 9 = 1\times 7+2; \\ 3-5 &= 5 \quad \bmod 7 \textit{ as } 3-5=-2 \textit{ and } -2 = (-1)\times 7+5; \\ 3\times 5 &= 1 \quad \bmod 7 \textit{ as } 3\times 5 = 15 \textit{ and } 15 = 2\times 7+1. \end{aligned}$$

We can more concisely write down all the rules of $\bmod 7$ *arithmetic with addition and multiplication tables:*

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Definition 125 has the advantage of being unambiguous (i.e. the operations $+, -, \times$ clearly deliver well-defined answers) but it also looks a little unnatural. For example, is it clear that the distributive law still applies? Alternatively, we can take a more formal view of what the arithmetic of $\mathbb{Z}_n$ is. In Proposition 112, we met the equivalence relation on $\mathbb{Z}$ given by $a \sim b$ if $a-b$ is a multiple of n. We can see now that this is the same as saying

$$a \sim b \text{ if and only if } a = b \quad \bmod n. \tag{4.1}$$

We saw in Example 116 that there are then n equivalence classes $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$. An alternative, more formal but also more natural, definition of the arithmetic of $\mathbb{Z}_n$ is then:

Definition 128 *Let $\mathbb{Z}_n$ denote the equivalence classes $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$ of $\mathbb{Z}$ under the equivalence relation (4.1). We define the operations $+$ and $\times$ on $\mathbb{Z}_n$ by*

$$\bar{a} + \bar{b} = \overline{a+b}, \qquad \bar{a} \times \bar{b} = \overline{a \times b}.$$

Proposition 129 *The operations $+$ and $\times$ are well-defined on $\mathbb{Z}_n$.*

Proof. How might + and × not be well-defined? Well, because the same equivalence class has many different representatives (e.g. $\bar{1} = \bar{7}$ in $\mathbb{Z}_6$) it's feasible that we might have $\bar{a} = \bar{\alpha}$ and $\bar{b} = \bar{\beta}$ yet $\overline{a+b} \neq \overline{\alpha+\beta}$. Adding the same two elements shouldn't be able to yield two different sums. So suppose that $\bar{a} = \bar{\alpha}$ and $\bar{b} = \bar{\beta}$, then

$$a - \alpha = kn \text{ and } b - \beta = ln$$

for $k, l \in \mathbb{Z}$. But then

$$(a+b) - (\alpha+\beta) = (a-\alpha) + (b-\beta) = (k+l)n$$

and

$$ab - \alpha\beta = (\alpha + kn)(\beta + ln) - \alpha\beta = (k\beta + l\alpha + kln)n$$

and hence $\overline{a+b} = \overline{\alpha+\beta}$ and $\overline{ab} = \overline{\alpha\beta}$ are both true so that + and × are well-defined. ■

Proposition 130 *(a) $(\mathbb{Z}_n, +)$ is an abelian group isomorphic to C_n.*
(b) Further × is associative, commutative and distributes over +.

Proof. That $(\mathbb{Z}_n, +)$ is an abelian group and the properties of × mentioned in (b) are all inherited from the same properties in $\mathbb{Z}$. For example, to see that the distributive law still holds, we simply have to note for $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ that

$$\begin{aligned}
\bar{a}\left(\bar{b} + \bar{c}\right) &= \bar{a}(\overline{b+c}) && [\text{as } + \text{ is well-defined in } \mathbb{Z}_n] \\
&= \overline{a(b+c)} && [\text{as } \times \text{ is well-defined in } \mathbb{Z}_n] \\
&= \overline{ab+ac} && [\text{by the distributive law in } \mathbb{Z}] \\
&= \overline{ab} + \overline{ac} && [\text{as } + \text{ is well-defined in } \mathbb{Z}_n] \\
&= \bar{a}\,\bar{b} + \bar{a}\,\bar{c} && [\text{as } \times \text{ is well-defined in } \mathbb{Z}_n].
\end{aligned}$$

To see that $(\mathbb{Z}_n, +)$ is indeed cyclic we need only note that $\bar{1}$ has (additive) order n. ■

We now note, for certain values of n, that modular arithmetic can have some unfortunate algebraic aspects such as

$$3 \times 5 = 0 \bmod 15, \qquad 4 \times 3 = 0 \bmod 6.$$

It follows that one cannot divide by 3 or 5 in $\mathbb{Z}_{15}$ nor divide by 3 or 4 in $\mathbb{Z}_6$. More generally we note:

Proposition 131 *Let $\bar{x} \in \mathbb{Z}_n$ with $x \neq 0$.*

(a) $\bar{x}$ has a multiplicative inverse if and only if $\operatorname{hcf}(x,n) = 1$. Hence if n is prime, then $\mathbb{Z}_n$ is in fact a field.

*(b) Those $\bar{x}$ with a multiplicative inverse (the so-called **units**) form a group $\mathbb{Z}_n^*$ under multiplication.*

Proof. This is left as Exercise Sheet 4, Question 2. ■

Example 132 *List the units in $\mathbb{Z}_{12}$. Identify the group $\mathbb{Z}_{12}^*$.*

Solution. As $12 = 2^2 \times 3$ then the units of $\mathbb{Z}_{12}$ are $1, 5, 7, 11$. Note that the group table is

$*$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

showing that $\mathbb{Z}_{12}^*$ is isomorphic to $C_2 \times C_2$. ■

5. ORDER. LAGRANGE'S THEOREM

Recall that we also defined the *order* $\mathrm{o}(g)$ of a group element:

Definition 133 *Let G be a group and $g \in G$. If there is a positive integer k such that $g^k = e$, then the **order** $\mathrm{o}(g)$ of $g \in G$ is defined as*

$$\mathrm{o}(g) = \min\{m > 0 \colon g^m = e\}.$$

Otherwise we say that the order of g is infinite.

Proposition 134 *If G is finite, then $\mathrm{o}(g)$ is finite for each $g \in G$.*

Proof. Consider the list

$$g, g^2, g^3, g^4, \ldots$$

As G is finite, then this list must have repeats. Hence there are integers $i > j$ such that $g^i = g^j$. So $g^{i-j} = e$ showing that $\{m > 0 \colon g^m = e\}$ is non-empty and so has a minimal element. ■

Proposition 135 *If $g \in G$ and $\mathrm{o}(g)$ is finite, then $g^n = e$ if and only if $\mathrm{o}(g)|n$.*

Proof. If $n = k\mathrm{o}(g)$ then

$$g^n = \left(g^{\mathrm{o}(g)}\right)^k = e^k = e.$$

Conversely, if $g^n = e$ then, by the division algorithm, there are integers q, r such that $n = q\mathrm{o}(g) + r$ where $0 \leqslant r < \mathrm{o}(g)$. Then

$$g^r = g^{n - q\mathrm{o}(g)} = g^n (g^{\mathrm{o}(g)})^{-q} = e.$$

By the minimality of $\mathrm{o}(g)$ then $r = 0$ and so $n = q\mathrm{o}(g)$. ■

Proposition 136 *If $\phi \colon G \to H$ is an isomorphism and $g \in G$ then $\mathrm{o}(\phi(g)) = \mathrm{o}(g)$.*

Proof. We have

$$(\phi(g))^k = e_H \iff \phi(g^k) = e_H \iff g^k = e_G$$

as ϕ is injective. ■

Example 137 *In D_8 we have*

$$\mathrm{o}(e) = 1, \quad \mathrm{o}(r^2) = \mathrm{o}(s) = \mathrm{o}(rs) = \mathrm{o}(r^2 s) = \mathrm{o}(r^3 s) = 2, \quad \mathrm{o}(r) = \mathrm{o}(r^3) = 4.$$

Proposition 138 *Let x, n be integers with $n \geqslant 2$. Then the order $\mathrm{o}(\bar{x})$ of $\bar{x} \in \mathbb{Z}_n$ is*

$$\mathrm{o}(\bar{x}) = \frac{n}{\mathrm{hcf}(x, n)}.$$

Proof. Left to Exercise Sheet 4, Question 1. ■

Corollary 139 *$\bar{x} \in \mathbb{Z}_n$ is a generator if and only if* $\operatorname{hcf}(x, n) = 1$.

Definition 140 *Let H be a subgroup of G.*
*Then the **left cosets** of H (or left H-cosets) are the sets*

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

*The **right cosets** of H (or right H-cosets) are the sets*

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

Notation 141 *We write G/H for the set of (left) cosets of H in G. The cardinality of G/H is called the **index** of H in G.*

Remark 142 *(i) Note that different elements g_1,$g_2 \in G$ can represent the same (left) coset – i.e. we can have $g_1H = g_2H$ yet $g_1 \neq g_2$.*

(ii) In general, we will have $gH \neq Hg$. Obviously we will have $gH = Hg$ if G is abelian, and in other cases as well.

Example 143 *Let $G = S_3$ and $H = \{e, (12)\}$. Then*

$$\begin{array}{rlrl} eH = (12)\,H &= \{e, (12)\}; & He = H\,(12) &= \{e, (12)\}; \\ (13)\,H = (132)\,H &= \{(13)\,, (132)\}; & H\,(13) = H\,(123) &= \{(13)\,, (123)\}; \\ (23)\,H = (123)\,H &= \{(23)\,, (123)\}; & H\,(23) = H\,(132) &= \{(23)\,, (132)\}. \end{array}$$

Note here that $Hg \neq gH$ in general.

Example 144 *Let $G = S_n$ and $H = A_n$. Then*

$$\sigma A_n = A_n\sigma = A_n \quad \text{when } \sigma \text{ is even;} \qquad \sigma A_n = A_n\sigma = S_n \backslash A_n \quad \text{when } \sigma \text{ is odd.}$$

Note that $\sigma A_n = A_n\sigma$ for all $\sigma \in S_n$, even though S_n is not (in general) abelian.

Example 145 *Let $G = \mathbb{C}^*$ and $H = S^1$. Then, for $w \in \mathbb{C}^*$, we have*

$$wS^1 = \{z \in \mathbb{C}^* \colon \ |z| = |w|\}.$$

Example 146 *Let $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Then the (left and right) coset of $r \in \mathbb{Z}$ is $r + n\mathbb{Z}$. So there are n cosets*

$$0 + n\mathbb{Z}, \quad 1 + n\mathbb{Z}, \quad 2 + n\mathbb{Z}, \quad \ldots \quad (n-1) + n\mathbb{Z} = -1 + n\mathbb{Z}.$$

So we can naturally identity $\mathbb{Z}_n$ with $\mathbb{Z}/n\mathbb{Z}$ (if only as sets for the moment).

Lemma 147 ***(Coset Equality Lemma)*** *Let $H \leqslant G$ and $g, k \in \dot{G}$. Then*

$$gH = kH \iff k^{-1}g \in H.$$

For right cosets, $Hg = Hk \iff kg^{-1} \in H$.

Proof. Suppose that $gH = kH$. Then $g = ge \in kH$ and so there exists $h \in H$ such that $g = kh$. Hence $k^{-1}g = h \in H$.

Conversely suppose that $k^{-1}g = h \in H$. Then $gH = khH \subseteq kH$ and $kH = g\left(g^{-1}k\right)H = gh^{-1}H \subseteq gH$. ■

Remark 148 *The relation on G given by $g \sim k \iff k^{-1}g \in H$ is an equivalence relation on G with the equivalence classes being the left cosets of H. This essentially comprises part of the following proof of Lagrange's Theorem when we prove that the (left) cosets partition G.*

Theorem 149 ***(Lagrange's Theorem)*** *(First instances of theorem due to Lagrange in 1771.)*
Let G be a finite group and H a subgroup of G. Then $|H|$ divides $|G|$.

Remark 150 *There are two steps to this proof. We shall prove:*
(a) The (left or right) cosets of H partition G.
(b) Each (left or right) coset of H is equinumerous with H.
Both (a) and (b) in fact hold for infinite groups.

Proof. Let G be a (not necessarily finite) group G and H a subgroup of G.

(a) For any $g \in G$, note $g = ge \in gH$, so that the union of the (left) cosets is G. Now suppose that two cosets aren't disjoint; we'll show that they must be equal. Say $k \in g_1H \cap g_2H$. Then there are $h_1, h_2 \in H$ such that $k = g_1h_1 = g_2h_2$. Then $g_2^{-1}g_1 = h_2h_1^{-1} \in H$ and $g_1H = g_2H$ by the Coset Equality Lemma.

(b) For any $g \in G$ then $h \mapsto gh$ is a bijection between H and gH. This map is clearly onto and also 1-1, for if $gh_1 = gh_2$ then we see $h_1 = h_2$ by applying g^{-1}. Hence $|gH| = |H|$.

Finally, if G is finite, then we have

$$|G| = |G/H| \times |H|$$

and hence $|H|$ divides $|G|$. ■

Remark 151 *Lagrange's Theorem states that the order of a subgroup is a factor of the order of the group. The converse does* ***not*** *hold – that is, if G is a finite group and k is a factor of $|G|$ then there need not be a subgroup H of G such that $|H| = k$. For example, $|A_4| = 12$ yet A_4 has no subgroup of order 6. (See Examples 86 and 209.) The converse of Lagrange's Theorem* ***is*** *true for cyclic groups though: for if k divides n then $\overline{n/k}$ has order k in $\mathbb{Z}_n$.*

Example 152 *Find all the subgroups of (i) $\mathbb{Z}_{31}$; (ii) D_{10}; (iii) $\mathbb{Z}_5 \times \mathbb{Z}_5$.*

Solution. (i) As 31 is prime then a subgroup must have order 1 or 31. Hence the only subgroups are $\{\bar{0}\}$ and $\mathbb{Z}_{31}$ itself.

(ii) The subgroups of D_{10} can have order $1, 2, 5$ or 10. So aside from $\{e\}$ and D_{10} we can have order 2 subgroups of the form $\{e, \text{ reflection}\}$ and the only order 5 subgroup consists of the five rotations.

(iii) $|\mathbb{Z}_5 \times \mathbb{Z}_5| = 25$. So the subgroups can have order $1, 5$ or 25. Every element in $\mathbb{Z}_5 \times \mathbb{Z}_5$ apart from $(\bar{0},\bar{0})$ has order 5. The subgroups of order 5 consist of the identity $(\bar{0},\bar{0})$ and four elements of order 5 each of which generate that subgroup. So there are $(25-1)/(5-1) = 6$ such subgroups. Specifically these are

$$\begin{array}{ll} \{(\bar{0},\bar{0}),(\bar{1},\bar{0}),(\bar{2},\bar{0}),(\bar{3},\bar{0}),(\bar{4},\bar{0})\}\,; & \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{0},\bar{3}),(\bar{0},\bar{4})\}\,; \\ \{(\bar{0},\bar{0}),(\bar{1},\bar{1}),(\bar{2},\bar{2}),(\bar{3},\bar{3}),(\bar{4},\bar{4})\}\,; & \{(\bar{0},\bar{0}),(\bar{1},\bar{2}),(\bar{2},\bar{4}),(\bar{3},\bar{1}),(\bar{4},\bar{3})\}\,; \\ \{(\bar{0},\bar{0}),(\bar{2},\bar{1}),(\bar{4},\bar{2}),(\bar{1},\bar{3}),(\bar{3},\bar{4})\}\,; & \{(\bar{0},\bar{0}),(\bar{1},\bar{4}),(\bar{2},\bar{3}),(\bar{3},\bar{2}),(\bar{4},\bar{1})\}\,. \end{array}$$

The only other subgroups are then $\{(\bar{0},\bar{0})\}$ and $\mathbb{Z}_5 \times \mathbb{Z}_5$. ■

Corollary 153 *Let G be a finite group and $g \in G$. Then $\mathrm{o}(g)$ divides $|G|$.*

Proof. $\langle g \rangle = \{e, g, g^2, \ldots, g^{\mathrm{o}(g)-1}\}$ is a subgroup of G with order $\mathrm{o}(g)$. ■

Remark 154 *This Corollary has no converse: for example, S_3 has no element of order 6. However we shall later prove Cauchy's Theorem which states that if p is a prime factor of $|G|$ then there is a group element with order p. We shall prove this for $p = 2$ (see Corollary 162 below).*

Corollary 155 *Let G be a finite group with $|G| = p$, a prime. Then G is cyclic.*

Proof. Let $g \in G$ with $g \neq e$. Then $\mathrm{o}(g) \neq 1$ and yet $\mathrm{o}(g)$ divides p, so $\mathrm{o}(g) = p$. Hence $|\langle g \rangle| = p$. That is $\langle g \rangle = G$ and G is cyclic. ■

Corollary 156 *Let G be a finite group and $g \in G$. Then $g^{|G|} = e$.*

Proof. $|G|$ is a multiple of $\mathrm{o}(g)$ and $g^{\mathrm{o}(g)} = e$. ■

Theorem 157 ***(Fermat's Little Theorem,** 1640) Let p be a prime and $a \in \mathbb{Z}$ such that p does not divide a. Then $a^{p-1} = 1 \bmod p$.*

Proof. This is just Corollary 156 with $G = \mathbb{Z}_p^*$ as $\left|\mathbb{Z}_p^*\right| = p - 1$. ■

Theorem 158 ***(Euler's Theorem,** 1736) Let $n \geqslant 2$ and let $a \in \mathbb{Z}$ be coprime with n. Then*

$$a^{\phi(n)} = 1 \bmod n$$

where $\phi(n) = |\{k\colon 0 < k < n, \mathrm{hcf}(k,n) = 1\}|$.

Proof. This is just Corollary 156 with $G = \mathbb{Z}_n^*$ as $\phi(n) = |\mathbb{Z}_n^*|$. ■

Remark 159 *(Off-syllabus) The "phi function" or "totient function" $\phi(n)$ was introduced by Euler in 1760. It is an important number-theoretic function with the following properties.*

(i) $\phi(p) = p - 1$ for a prime p.

(ii) $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

(iii) $\phi(mn) = \phi(m)\phi(n)$ if m and n are coprime.

Lemma 160 *Let G be a group. Then the relation $\sim$ on G defined by*

$$x \sim y \iff x = y \quad or \quad x = y^{-1}$$

is an equivalence relation. The equivalence classes are generally of the form $\bar{x} = \{x, x^{-1}\}$ unless x is self-inverse in which case $\bar{x} = \{x\}$.

Proof. Left as an exercise. ■

Corollary 161 ***(Wilson's Theorem)*** *If p is a prime then*

$$(p-1)! = -1 \mod p.$$

Proof. If $p = 2$ then this just says $1 = -1 \mod 2$ which is true. So assume $p \geqslant 3$. Consider the self-inverse elements in $\mathbb{Z}_p^*$. We see

$$\bar{x} = \bar{x}^{-1} \iff \bar{x}^2 = 1 \iff (\bar{x} - \bar{1})(\bar{x} + \bar{1}) = \bar{0} \iff \bar{x} = \bar{1} \text{ or } \bar{x} = -\bar{1}$$

as $\mathbb{Z}_p$ is a field. So the only singleton equivalence classes of $\sim$ (the equivalence relation defined in Lemma 160) are $\{\bar{1}\}$ and $\{-\bar{1}\}$ with all others being of the form $\{\bar{x}, \bar{x}^{-1}\}$. As the equivalence classes partition $\mathbb{Z}_p^*$ then

$$(p-1)! = \prod_{\bar{k} \in \mathbb{Z}_p^*} \bar{k} = \prod_{\substack{\text{equivalence}\\ \text{classes}}} \prod_{\substack{\text{each}\\ \text{equivalence}\\ \text{class}}} \bar{k} = \bar{1} \times (-\bar{1}) \times \prod_{\substack{\text{doubleton}\\ \text{equivalence}\\ \text{classes}}} \bar{k} = -\bar{1}$$

as the contribution to the product from each doubleton equivalence class is $\bar{x} \times \bar{x}^{-1} = \bar{1}$. ■

Corollary 162 *Let G be a group with even order. Then G has an element of order* 2.

Proof. Consider the equivalence relation on G defined in Lemma 160. If there are m doubleton equivalence classes and n singleton equivalence classes, then we have

$$2m + n = |G|$$

as the equivalence classes partition $|G|$. As $|G|$ is even then n is even but we also know $n \geqslant 1$ as e is self-inverse. So, in fact, $n \geqslant 2$ and there is a non-identity element x which satisfies $x = x^{-1}$ or equivalently $x^2 = e$ so that $\mathrm{o}(x) = 2$. ■

Theorem 163 *Let G be a finite group with $|G| = 2p$ where $p \geqslant 3$ is prime. Then G is isomorphic to C_{2p} or D_{2p}.*

Proof. Assume that G is not cyclic. The possible orders of elements in G are 1 (the identity e) or 2 or p. As $|G| = 2p$ is even then there is an element $x \in G$ of order 2. (Corollary 162). Further if $g^2 = e$ for all $g \in G$ then $G \cong (\mathbb{Z}_2)^n$ for some n (Exercise Sheet 4, Question 5), which is not possible here and hence there is an element $y \in G$ of order p. As x has order 2 and $y, y^2, \ldots, y^{p-1}$ have order p then $x \notin \langle y \rangle$. Hence $G = \langle y \rangle \cup x\langle y \rangle$ or more expansively

$$G = \left\{e, y, y^2, \ldots, y^{p-1}, x, xy, xy^2, \ldots, xy^{p-1}\right\}.$$

Now the product yx is somewhere amongst G. If $yx = y^i$ we arrive at a similar contradiction to before. So $yx = xy^j$ for some $1 \leqslant j < p$. Then

$$(yx)^2 = yxyx = (yx)\left(xy^j\right) = y^{j+1}; \qquad (yx)^3 = \left(xy^j\right)(yx)^2 = xy^{2j+1};$$

until more generally we find that $(yx)^{2k} = y^{k(j+1)}$ and that $(yx)^{2k+1} = xy^{kj+k+j}$. So yx has an even order and $\mathrm{o}\,(yx) = 2$. In particular it follows that $j = p - 1$. Hence

$$G = \langle x, y \colon x^2 = y^p = e, yx = xy^{p-1} \rangle$$

which is a *presentation* for D_{2p}. We can think of x as reflection in a given axis and y as clockwise rotation through $2\pi/p$. ■

Remark 164 *(Off Syllabus)* ***Presentations.*** *Recall that the dihedral group D_{2n} can be defined as*

$$D_{2n} = \langle r, s \colon r^n = e = s^2, sr = r^{-1}s \rangle. \tag{5.1}$$

Equation (5.1) is an example of a **presentation** *for D_{2n}. We can think of r as a rotation and s as a reflection if we want to make real the elements r and s, but there's no great need as the presentation contains everything necessary to describe the algebra of D_{2n} or any group isomorphic to D_{2n}. A presentation of a group describes some* ***generators*** *of the group (here r and s) and the (non-trivial) rules or* ***relations*** *that govern the algebra in the group. Contained in the relations is enough information to show that the group contains $2n$ elements $e, r, , \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s$ and determine products between them. Any other string or* ***word*** *in the generators can be shown to be one of these $2n$ elements by means of the relations. For example, we can see that*

$$sr^3sr^2s = \left(sr^3\right)sr^2s = r^{-3}(ss)\,r^2s = r^{-1}s = r^{n-1}s.$$

Other group presentations include

$$\mathbb{Z} \cong \langle g \rangle, \qquad C_n \cong \langle g \colon g^n = e \rangle, \qquad \mathbb{Z}^2 \cong \langle g, h \colon gh = hg \rangle.$$

There are, of course, many different ways to present the same group. Note $a = s$ and $b = rs$ generate D_6. We can write the other elements as

$$r^2 = ab, \qquad r = ba, \qquad r^2s = aba$$

and see that

$$D_6 = \langle a, b \colon a^2 = e = b^2, bab = aba \rangle.$$

We need to check we have enough relations. Using the relations $a^2 = e = b^2$ we see that we need only consider those strings (or words) which alternately go a then b. And using the relation $bab = aba$ we can contract substrings of bab from longer words via

$$a\,(bab) = a\,(aba) = ba, \qquad (bab)\,a = (aba)\,a = ab.$$

The only strings that can't be contracted further in this way are e, a, b, ab, ba, aba.

6. HOMOMORPHISMS AND ISOMORPHISMS

Let G and H be groups. Recall that an **isomorphism** $\phi\colon G \to H$ is a bijection such that

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2) \quad \text{for all } g_1, g_2 \in G.$$

We say that two groups, G and H, are **isomorphic,** and write $G \cong H$, if there is an isomorphism between the groups. Two isomorphic groups should usually be considered as manifestations of the same group. We proved in the first half of the course that:

Theorem 165 *Let G be a group with $|G| = p$, a prime. Then $G \cong C_p$.*

Theorem 166 *Let G be a group with $|G| = 2p$ where $p \geqslant 3$ is prime. Then $G \cong C_{2p}$ or $G \cong D_{2p}$.*

These results are sufficient to demonstrate the following:

Theorem 167 *Up to isomorphism, the groups of order $\leqslant 7$ are:*

- *Order 2: C_2*
- *Order 3: C_3*
- *Order 4: C_4 or $C_2 \times C_2 \cong V_4$*
- *Order 5: C_5*
- *Order 6: C_6 or $S_3 \cong D_6$*
- *Order 7: C_7*

The general situation (re how many groups there are of a give order n) is very complicated and depends largely on the factors of n. Even the $n = 8$ case (stated below) is more complicated and beyond the scope of this first course.

Theorem 168 *Up to isomorphism, the groups of order 8 are*

$$C_8, \qquad C_2 \times C_4, \qquad C_2 \times C_2 \times C_2, \qquad D_8, \qquad Q_8.$$

Remark 169 *We have yet to meet the fifth group Q_8 which is usually introduced via the quaternions. A **quaternion** might be thought of as a four-dimensional version of a complex number. A quaternion is a number of the form*

$$q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \qquad (a, b, c, d \in \mathbb{R})$$

with quaternions adding as one might expect and multiplying distributively and associatively according to the rules

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1.$$

An example of the group Q_8 is then

$$Q_8 = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}.$$

The equivalent of a linear map in group theory is the homomorphism.

Definition 170 *Let G and H be groups. A* ***homomorphism*** $\phi\colon G \to H$ *is a map such that*

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2) \quad \textit{for all } g_1, g_2 \in G.$$

Hence an ***isomorphism*** *between G and H is simply a bijective homomorphism.*

We also have:

Definition 171 *An* ***automorphism*** *of a group G is an isomorphism from G to G. The automorphisms of G form a group* $\mathrm{Aut}(G)$ *under composition. (Exercise Sheet 5, Question 5).*

An ***endomorphism*** *of G is a homomorphism from G to G.*

(Rarely used) A ***monomorphism*** *is an injective homomorphism and an* ***epimorphism*** *is a surjective homomorphism.*

Homomorphisms in group theory have many properties akin to linear maps in linear algebra.

Proposition 172 *Let $\phi\colon G \to H$ be a homomorphism between groups and let $g \in G$, $n \in \mathbb{Z}$. Then*

$$\textit{(i)} \quad \phi(e_G) = e_H. \qquad \textit{(ii)} \quad \phi(g^{-1}) = (\phi(g))^{-1}. \qquad \textit{(iii)} \quad \phi(g^n) = (\phi(g))^n.$$

Proof. (i) We have $\phi(e_G) = \phi(e_G * e_G) = \phi(e_G)\phi(e_G)$ and applying $\phi(e_G)^{-1}$ to both sides (i) follows. For (ii) note

$$\phi(g)\,\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_G) = e_H$$

demonstrating (ii). For (iii) note more generally that we can show $\phi(g^n) = (\phi(g))^n$ for $n > 0$ by induction and then for $n = -k < 0$ we have

$$\phi(g^n) = \phi((g^{-1})^k) = (\phi(g^{-1}))^k = (\phi(g)^{-1})^k = \phi(g)^n.$$

■

Corollary 173 *Let $\phi\colon G \to H$ be a homomorphism between groups and let $g \in G$. Then* $\mathrm{o}(\phi(g))$ *divides* $\mathrm{o}(g)$.

Proof. Note

$$\phi(g)^{\mathrm{o}(g)} = \phi(g^{\mathrm{o}(g)}) = \phi(e_G) = e_H.$$

In a group, $k^n = e$ if and only if n is a multiple of $\mathrm{o}(k)$ (by Proposition 135). ■

Example 174 *The map $\phi\colon \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(n) = \bar{n}$ is a homomorphism as*

$$\overline{m+n} = \overline{m} + \overline{n}.$$

Example 175 *If H is a subgroup of G then* ***inclusion*** $\iota\colon H \to G$ *given by $\iota(h) = h$ is a homomorphism.*

Example 176 *For any groups G, H the map $\phi\colon G \to H$ given by $\phi(g) = e_H$ is a group homomorphism.*

Example 177 *Let G_1 and G_2 be groups. Then the maps*

$$\pi_1\colon G_1 \times G_2 \to G_1, \quad (g_1, g_2) \mapsto g_1 \quad \textit{and} \quad \pi_2\colon G_1 \times G_2 \to G_2, \quad (g_1, g_2) \mapsto g_2$$

are homomorphisms.

Example 178 *The map* $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ *given by*

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \textit{if } \sigma \textit{ is even} \\ -1 & \textit{if } \sigma \textit{ is odd} \end{cases}$$

is a homomorphism as, for $\sigma, \tau \in S_n$, we have $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.

Example 179 *The map* $\det\colon GL(n, \mathbb{R}) \to \mathbb{R}^*$ *is a homomorphism as, for $n \times n$ matrices A, B we have* $\det(AB) = \det A \det B$.

Example 180 *The map* $\operatorname{trace}\colon M_n(\mathbb{R}) \to \mathbb{R}$ *is a homomorphism as, for $n \times n$ matrices A, B we have* $\operatorname{trace}(A + B) = \operatorname{trace} A + \operatorname{trace} B$.

Example 181 *The map* $\log\colon (0, \infty) \to \mathbb{R}$ *is a homomorphism as for $x, y > 0$ we have* $\log(xy) = \log x + \log y$. *In fact, being a bijection, this is an isomorphism.*

Example 182 *The map $\phi\colon \mathbb{R} \to S^1$ given by $\phi(x) = e^{ix}$ is a surjective homomorphism as $e^{i(x+y)} = e^{ix}e^{iy}$.*

Example 183 *The map $\phi\colon \mathbb{C}^* \to \mathbb{R}^*$ given by $\phi(z) = |z|$ is a group homomorphism as $|zw| = |z|\,|w|$ for $z, w \neq 0$.*

Example 184 *The map $\phi\colon \mathbb{R}^* \to \mathbb{R}^*$ given by $\phi(x) = x^2$ is a group homomorphism as $(xy)^2 = x^2y^2$.*

Remark 185 *More generally $\phi\colon G \to G$ given by $\phi(g) = g^2$ is a homomorphism if and only if G is abelian. (This is left as an exercise).*

Proposition 186 *Let $a \in G$, a group. Conjugation by a, i.e. the map $\theta_a\colon G \to G$ given by $\theta_a(g) = a^{-1}ga$ is an isomorphism.*

Proof. Firstly we note

$$\theta_a(gh) = a^{-1}gha = (a^{-1}ga)(a^{-1}ha) = \theta_a(g)\theta_a(h).$$

Secondly an easy check shows that $\theta_{a^{-1}} = (\theta_a)^{-1}$ and so θ_a is a bijection. ■

Corollary 187 *Let G be a group and $g, h \in G$.*
(i) If g and h are conjugate then $\mathrm{o}(g) = \mathrm{o}(h)$.
(ii) If g and h are conjugate then g^{-1} and h^{-1} are conjugate.

Proposition 188 *Homomorphisms $\phi\colon \mathbb{Z} \to \mathbb{Z}$ are all of the form $\phi(x) = nx$ for some $n \in \mathbb{Z}$.*

Proof. Certainly, for any $n \in \mathbb{Z}$, we have that $\phi(x) = nx$ is a homomorphism as

$$\phi(x+y) = n(x+y) = nx + ny = \phi(x) + \phi(y).$$

Conversely, for any homomorphism $\phi\colon \mathbb{Z} \to \mathbb{Z}$, if we set $n = \phi(1)$ then by Proposition 172 (iii) we have for $x > 0$

$$\phi(x) = \phi\left(\underbrace{1 + 1 + \cdots + 1}_{x \text{ times}}\right) = \underbrace{\phi(1) + \phi(1) + \cdots + \phi(1)}_{x \text{ times}} = nx$$

and then $\phi(-x) = -\phi(x) = -nx = n(-x)$. ■

Remark 189 *As a crucial aspect of the above proof we have just noted that, if G is a cyclic group with generator g, then any homomorphism from G is entirely determined by the value of $\phi(g)$ as*

$$\phi(g^r) = (\phi(g))^r \quad \text{for any } r \in \mathbb{Z}.$$

More generally if $g_1, \ldots, g_k$ are generators of a group G then any homomorphism from G is entirely determined by the values $\phi(g_1), \ldots, \phi(g_k)$.

This result corresponds to the similar result in linear algebra: any linear map $T\colon V \to W$ is determined by the values T takes on a basis of V (or more generally on a spanning set).

In a comparable way to linear maps, we can also define the kernel and image of a homomorphism. As one might expect from the study of linear maps, kernels and images in group theory are subgroups – in fact, more than this, kernels turn out to be a special type of subgroup.

Definition 190 *Let $\phi\colon G \to H$ be a homomorphism between groups. Then:*
*(i) the **kernel** of ϕ, written* $\ker\phi$, *equals*

$$\ker\phi = \{g \in G \colon \phi(g) = e_H\} \subseteq G.$$

*(ii) the **image** of ϕ, written* $\operatorname{Im}\phi$, *equals*

$$\operatorname{Im}\phi = \{\phi(g) \colon g \in G\} \subseteq H.$$

Definition 191 *Let G be a group and H a subgroup of G. Then H is said to be a **normal subgroup of** G if*

$$gH = Hg \qquad \text{for all } g \in G$$

or equivalently if

$$g^{-1}hg \in H \qquad \text{for all } g \in G,\ h \in H.$$

If H is a normal subgroup of G then we write $H \lhd G$.

Proposition 192 *Let $\phi\colon G \to H$ be a homomorphism between two groups. Then* $\ker\phi \lhd G$.

Proof. Say $k_1, k_2 \in \ker\phi$ and $g \in G$. Then

$$\phi(e_G) = e_H; \qquad \phi(k_1k_2) = \phi(k_1)\phi(k_2) = e_He_H = e_H; \qquad \phi(k_1^{-1}) = \phi(k_1)^{-1} = e_H^{-1} = e_H$$

showing that $\ker\phi$ is a subgroup of G; further as

$$\phi(g^{-1}k_1g) = \phi(g^{-1})\phi(k_1)\phi(g) = \phi(g)^{-1}e_H\phi(g) = e_H$$

then $\ker\phi$ is a normal subgroup of G. ■

Proposition 193 *Let* $\phi\colon G \to H$ *be a homomorphism between two groups. Then* $\operatorname{Im}\phi \leqslant H$;

Proof. Note $e_H = \phi(e_G) \in \operatorname{Im}\phi$. Say $h_1, h_2 \in \operatorname{Im}\phi$. Then there are g_i such that $\phi(g_i) = h_i$. Note

$$h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) \in \operatorname{Im}\phi; \qquad h_1^{-1} = \phi(g_1)^{-1} = \phi(g_1^{-1}) \in \operatorname{Im}\phi.$$

■

Example 194 *The map* $\phi\colon \mathbb{Z} \to \mathbb{Z}_n$ *given by* $\phi(n) = \bar{n}$ *has kernel* $n\mathbb{Z}$ *and has image* $\mathbb{Z}_n$.

Example 195 *The map* $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ *has kernel* A_n *and image* $\{\pm 1\}$.

Example 196 *The map* $\det\colon GL(n,\mathbb{R}) \to \mathbb{R}^*$ *has kernel* $SL(n,\mathbb{R})$ *and image* $\mathbb{R}^*$.

Example 197 *The map* $\phi\colon \mathbb{R} \to S^1$ *given by* $\phi(x) = e^{ix}$ *has kernel* $2\pi\mathbb{Z}$ *and image* $S^1.\phi$

Example 198 *The map* $\phi\colon \mathbb{C}^* \to \mathbb{R}^*$ *given by* $\phi(z) = |z|$ *has kernel* S^1 *and image* $(0,\infty)$.

We close this chapter with the following result – it is our first step to understanding homomorphisms via the First Isomorphism Theorem.

Proposition 199 *A homomorphism is constant on a coset of* $\ker\phi$ *and takes different values on different cosets.*

Proof.

$$\phi(g_1) = \phi(g_2) \iff \phi(g_2^{-1}g_1) = e_H \iff g_2^{-1}g_1 \in \ker\phi \iff g_1\ker\phi = g_2\ker\phi.$$

■

Corollary 200 *Let* $\phi\colon G \to H$ *be a homomorphism between two groups. Then* ϕ *is 1-1 if and only if* $\ker\phi = \{e_G\}$.

7. NORMAL SUBGROUPS. QUOTIENT GROUPS

Notation 201 *If $H \leqslant G$, then we write G/H for the set of (left) cosets of H in G.*

Let H be a subgroup of G. Recall that we say that H is a **normal** subgroup of G if

$$gH = Hg \text{ for all } g \in G$$

or equivalently if

$$g^{-1}hg \in H \text{ for all } g \in G, \; h \in H.$$

If H is a normal subgroup of G we write this $H \lhd G$.

Remark 202 *This does* ***NOT*** *mean that $gh = hg$ for all $g \in G$ and $h \in H$ or that G is abelian. Although we can easily see that all subgroups of abelian groups* ***are*** *normal.*

Remark 203 *H being a normal subgroup of G is a property of how H is contained in G and not solely a property of H. For example, if we consider $H = \langle (12) \rangle \leqslant S_3$ then H* ***is*** *normal in H but H is* ***not*** *normal in S_3.*

Remark 204 *In any group G, it is the case that $\{e\}$ and G are normal subgroups of G. If these are the only ones then G is said to be* ***simple****.*

Remark 205 *If asked to show that H is a normal subgroup of G then this means showing that both H is a subgroup of G* ***and*** *checking that H is normal in G.*

Remark 206 *Note that a subgroup $H \leqslant G$ is normal in G if and only if H is a union of conjugacy classes.*

Proposition 207 *Let $H \leqslant G$. If $|G/H| = 2$ then $H \lhd G$.*

Proof. Note that $eH = H = He$. So one left coset of H is H and one right coset of H is H. As there are only two (left or right) cosets, and as (left or right) cosets partition G then the other left coset is H^c (the complement of H in G) and the other right coset is also H^c. Recall that $gH = H$ if and only if $g \in H$ and likewise $Hg = H$ if and only if $g \in H$. Hence

$$\begin{aligned} \text{if } g &\in H \text{ then } gH = H = Gg; \\ \text{if } g &\notin H \text{ then } gH = H^c = Hg. \end{aligned}$$

■

Example 208 *For $n \geqslant 2$, this shows A_n is normal in S_n. Also $SO(n)$ is normal in $O(n)$.*

Example 209 *A_4 has no subgroup of order 6. In particular, Lagrange's Theorem has no converse.*

Solution. From Example 86, we know that the conjugcay classes of A_4 have sizes $1, 3, 4, 4$. If A_4 had a subgroup of order $6 = \frac{1}{2}|A_4|$ then it would be normal and hence a union of conjugacy classes. However no selection of $1, 3, 4, 4$ adds up to 6 so there is no subgroup of that order. ■

Example 210 *(a) The normal subgroups of S_3 are $\{e\}, A_3$ and S_3.*

(b) The normal subgroups of S_4 are $\{e\}, V_4, A_4$ and S_4.

Solution. (a) Recall that a normal subgroup is a union of conjugacy classes. The identity and the 2-cycles do not form a subgroup. The identity and the 3-cycles form A_3.

(b) The conjugacy classes e, (ab), (abc), $(abcd)$, $(ab)(cd)$ have respective sizes $1, 6, 8, 6, 3$. As the order of any subgroup is a factor of 24, this can only be achieved with these numbers as

$$1, \quad 1+3, \quad 1+8+3, \quad 1+6+8+6+3,$$

which correspond to the subgroups $\{e\}, V_4, A_4$ and S_4. ■

Definition 211 *Let G be a group. The **centre** of G, denoted $Z(G)$, is the set*

$$Z(G) = \{g \in G \colon gh = hg \ \text{ for all } h \in G\}.$$

Proposition 212 *Let G be a group. Then $Z(G) \lhd G$.*

Proof. (i) Certainly $eh = h = he$ for all $h \in G$ and so $e \in Z(G)$.

(ii) If $g_1, g_2 \in Z(G)$ and $h \in G$ then $(g_1g_2)h = g_1hg_2 = h(g_1g_2)$ and so $g_1g_2 \in Z(G)$.

(iii) If $g \in Z(G)$ and $h \in G$ then $gh = hg \implies hg^{-1} = g^{-1}h$ and so $g^{-1} \in Z(G)$.

(iv) Finally if $g \in Z(G)$ and $h \in G$, then $h^{-1}gh = h^{-1}hg = g \in Z(G)$. ■

Remark 213 *Note that $g \in Z(G)$ if and only if the conjugacy class of g is $\{g\}$.*

Example 214 *(a) If $n \geqslant 3$ then $Z(S_n) = \{e\}$.*
(b) The centre of $GL(n, F)$ is $\{\lambda I_n \colon \lambda \neq 0\}$.
(c) The centre of

$$D_{2n} = \langle r, s \colon r^n = s^2 = e,\ r^{-1}s = sr\rangle$$

is $\{e\}$ when n is odd and $\{e, r^{n/2}\}$ when n is even.

Solution. (a) and (b) will not be proved here. They are tractable but non-trivial exercises. (c) follows from Exercise Sheet 5, Question 3 and Remark 213. ■

Proposition 215 *Let $H \leqslant G$.*

(a) The binary operation $*$ on G/H given by

$$(g_1H) * (g_2H) = (g_1g_2)H$$

is well-defined if and only if $H \lhd G$.

(b) If $H \lhd G$ then $(G/H, *)$ is a group.

Definition 216 *If $H \lhd G$ then $(G/H, *)$ is called the **quotient group**.*

Proof. (a) Suppose that $H \lhd G$. Say $g_1 H = k_1 H$ and $g_2 H = k_2 H$, so that $k_1^{-1} g_1 \in H$ and $k_2^{-1} g_2 \in H$. We wish to show $(g_1 g_2) H = (k_1 k_2) H$. Note

$$\begin{aligned} (g_1 g_2) H = (k_1 k_2) H &\iff (k_1 k_2)^{-1} (g_1 g_2) \in H \\ &\iff k_2^{-1} k_1^{-1} g_1 g_2 \in H \\ &\iff k_2^{-1} \left(k_1^{-1} g_1\right) k_2 \left(k_2^{-1} g_2\right) \in H. \end{aligned}$$

We have already noted that $k_2^{-1} g_2 \in H$ and $k_1^{-1} g_1 \in H$; as H is normal then $k_2^{-1} \left(k_1^{-1} g_1\right) k_2 \in H$ also.

Conversely, suppose that $*$ is well-defined. Let $h \in H$ and $g \in G$. Then

$$\begin{aligned} \left(g^{-1} h g\right) H &= \left(g^{-1} H\right) * (hH) * (gH) \\ &= \left(g^{-1} H\right) * (eH) * (gH) \\ &= \left(g^{-1} e g\right) H \\ &= eH = H \end{aligned}$$

and in particular $g^{-1} h g \in H$. That is, H is a normal subgroup of G.

(b) Suppose now that $H \lhd G$. Then part (i) has shown that $*$ is a well-defined binary operation on G/H. Further $*$ is clearly associative as G's group operation is associative. Finally, we note that for any $g \in G$,

$$(eH) * (gH) = gH = (gH) * (eH)$$

and hence $eH = H$ is the identity element of G/H and for any $g \in G$

$$\left(g^{-1} H\right) * (gH) = eH = \left(g^{-1} H\right) * (gH)$$

so that

$$(gH)^{-1} = g^{-1} H \text{ in } G/H.$$

■

Remark 217 *Quotient Structures appear throughout pure mathematics. For a set S, then we can take an equivalence relation $\sim$ on S and consider the set of equivalence classes $S/\sim$. This is an example of a quotient structure with sets. Why might we ever want to do this? We do it all the time and have been doing so for some time. If asked the question, "what is the area of a triangle?" we respond "half base times height". We do not ask for the triangle's coordinates in $\mathbb{R}^2$, which would be "too much" information and just clutter the issue, but instead we are already thinking about the triangle's equivalence class under congruence because the answer is most naturally given in this format. So quotient structures can be a means of throwing away extraneous information and focussing on the most relevant information. As an example: can* $1,000,003$ *be written as the sum of two squares? At first glance this looks like it might be hard and something we need to resolve with the help of a computer. Solving the equation*

$$x^2 + y^2 = 1,000,003$$

looks fairly impenetrable but taking this equation in $\bmod 4$ *and showing that* $\bar{x}^2 + \bar{y}^2 = \bar{3}$ *has no solutions (rather easy as* $\bar{x}^2 = \bar{0}$ *or* $\bar{1}$ *for* $\bar{x} \in \mathbb{Z}_4$*) shows that the original equation had no solutions. By moving to* $\bmod 4$ *we have thrown away a lot of information but have reduced the problem in size and have crucially kept enough of the right information that conclusions can be still made about the original problem.*

Of course, with sets, we start off with rather structureless objects, so there aren't really any expectations of a structure on $S/\sim$. This is no longer the case when we look to make quotient groups and hope that a binary operation on the quotient might naturally arise from the binary operation on the original group.

Remark 218 *So if we have a group* G *and plan to make some elements equivalent, but still hope to have some sensible algebra afterwards, how should we go about this? We have met some of these ideas already with modular arithmetic. If we wish to introduce new rules, for example as in* $\mathbb{Z}_3$ *when we wish to say that* $3 \sim 0$*, then surely there will need to be further consequences of this rule if the resulting algebra is to be sensible. So we'd likewise expect:*

$$3 + 3 \sim 0 + 0 = 0 \quad \textit{and} \quad -3 \sim -0 = 0.$$

So, reasoning more generally, those elements which are equivalent to the identity will need to form a subgroup. More than that in fact (a point which is less obvious with the abelian example of $\mathbb{Z}_3$ *above) we will need that*

$$\textit{if } h \sim e \textit{ and } g \in G \textit{ then } g^{-1}hg \sim g^{-1}eg = e.$$

The equivalence class of e *will need to be a normal subgroup. From what we've seen earlier (Proposition 215) this is then sufficient for* $G/\sim$ *to be a well-defined group.*

In light of these comments it may be easier to think of G/H *as* $G \bmod H$*. From this viewpoint* H *is the equivalence class of* e *and we should think of* gH *as* $\bar{g}$*, the equivalence class of* g *instead. The somewhat cumbersome equation*

$$g_1H * g_2H = (g_1g_2)\,H \quad \textit{becomes} \quad \overline{g_1} * \overline{g_2} = \overline{g_1g_2}$$

which looks more natural and we see elements (or their equivalence classes) just multiply the way they did before and do so in a well-defined fashion.

Proposition 219 *Let* G *be a group and* H *a subset of* G*. Then* H *is a normal subgroup of* G *if and only if it is the kernel of some homomorphism from* G*.*

Proof. Suppose that H is the kernel of some homorphism $\phi\colon G \to K$. Then $H = \ker\phi$ is a normal subgroup by Proposition 192. Conversely if H is normal in G then

$$\pi\colon G \to G/H \qquad \text{given by } \pi(g) = gH$$

is a homomorphism with kernel H. This follows as

$$\pi(g_1g_2) = (g_1g_2)\,H = (g_1H)\,(g_2H) = \pi(g_1)\pi(g_2)$$

and

$$\pi(g) = H \iff gH = H \iff g \in H.$$

■

Example 220 *Let $G = \mathbb{Z}$ and $H = n\mathbb{Z}$ then*

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

and can naturally be identified with $\mathbb{Z}_n = \left\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\right\}$, the integers $\operatorname{mod} n$.

Example 221 *Let $G = S_n$ and $H = A_n$. Then*

$$S_n/A_n = \{A_n, S_n \backslash A_n\} = \{\textit{evens, odds}\} \cong C_2.$$

Example 222 *Let $G = D_{2n}$ and $H = \langle r \rangle$. Then $D_{2n}/\langle r \rangle \cong C_2$. We have "modded out" by so much that all that remains is a memory of whether the group element kept the polygon the same side up or flipped the polygon over.*

Example 223 *Let $G = \mathbb{C}^*$ and $H = S^1$. Then*

$$\mathbb{C}^*/S^1 \cong (0, \infty)$$

and this time we essentially "modded out" any details about argument with all elements on the circle $|z| = r$ being made equivalent to r.

Example 224 *As a further example*

$$S_4/V_4 \cong S_3.$$

See Exercise Sheet 6, Question 5.

Example 225 *Let $G = AGL(n, \mathbb{R})$ denote the group of affine maps*

$$f(\mathbf{x}) = A\mathbf{x} + \mathbf{b}, \qquad A \in GL(n, \mathbb{R}) \text{ and } \mathbf{b} \in \mathbb{R}^n$$

and T denote the subgroup of translations $t(\mathbf{x}) = \mathbf{x} + \mathbf{c}$. Then $T \lhd G$ and $G/T \cong GL(n, \mathbb{R})$.

Solution. This follows as

$$f^{-1}tf(\mathbf{x}) = f^{-1}t\,(A\mathbf{x} + \mathbf{b}) = f^{-1}(A\mathbf{x} + \mathbf{b} + \mathbf{c}) = A^{-1}((A\mathbf{x} + \mathbf{b} + \mathbf{c}) - \mathbf{b}) = \mathbf{x} + A^{-1}\mathbf{c}$$

and we can naturally identify fT with A to show the isomorphism $G/T \cong GL(n, \mathbb{R})$. ■

Example 226 *Let $n = 2k$ be even and let $G = D_{2n}$ and $H = Z(D_{2n}) = \left\{e, r^k\right\}$ noting that r^k is a half turn. Then*

$$D_{2n}/\langle r^k \rangle = \left\{\bar{e}, \bar{r}, \bar{r}^2, \ldots \bar{r}^{k-1}, \bar{s}, \bar{r}\bar{s}, \ldots, \bar{r}^{k-1}\bar{s}\right\}$$

where

$$\bar{r}^k = \bar{s}^2 = \bar{e} \quad \text{and} \quad \bar{s}\bar{r} = \bar{r}^{-1}\bar{s}$$

which is a presentation of D_n when $k \geqslant 3$ and is a presentation of V_4 when $k = 2$. So

$$D_{2n}/\langle r^{n/2} \rangle \cong D_n \quad (\text{for } n \geqslant 6) \text{ and } D_8/\langle r^2 \rangle \cong V_4.$$

The real importance of quotient groups will become more apparent when we meet the First Isomorphism Theorem.

7.1 Congruences (Off-syllabus)

There is another way of introducing quotient groups and that is via *congruences.*

Definition 227 *Let G be a group and $\sim$ an equivalence relation on G. Then we say that $\sim$ is a **congruence** if*
(i) whenever $g_1 \sim h_1$ and $g_2 \sim h_2$ then $g_1 g_2 \sim h_1 h_2$.
(ii) whenever $g \sim h$ then $g^{-1} \sim h^{-1}$.

So a congruence is an equivalence relation which respects the group operations. We have met examples of congruences already such as $= \mod n$. It is more apparent from this definition that $G/\sim$ will be a well-defined group in a natural way.

Proposition 228 *Let $\sim$ be a congruence on a group G. Then the congruence classes $G/\sim$ naturally form a group under the group operation $\bar{g} * \bar{h} = \overline{gh}$ where $\bar{g}$ denotes the congruence class of g.*

Proof. $*$ is a well-defined binary operation from (i) in the definition above. Associativity in $G/\sim$ is inherited from associativity in G and we also easily see $e_{G/\sim} = \bar{e}$ and $(\bar{g})^{-1} = \overline{g^{-1}}$. ■

The following propositions show that introducing quotient groups via congruences is entirely equivalent to introducing them via normal subgroups.

Proposition 229 *Let $H \leqslant G$. Then the equivalence relation $g \sim k \iff gH = kH$ is a congruence if and only if H is normal.*

Proof. Suppose that $\sim$ is a congruence and that $h \in H, g \in G$. Then $h \sim e$ and so, as $\sim$ is a congruence, $g^{-1}hg \sim g^{-1}eg = e$ showing that $g^{-1}hg \in H$. Conversely suppose that $H \lhd G$. Then $\sim$ is a congruence by Proposition 215. ■

Proposition 230 *Let $\sim$ be a congruence on group G. Then*
(a) $\bar{e}$ is a normal subgroup of G.
(b) $G/\sim$ is isomorphic to $G/\bar{e}$.

Proof. (a) Clearly $e \in \bar{e}$. If $h, k \in \bar{e}$ then, as $\sim$ is a congruence,

$$h^{-1}k \sim e^{-1}e = e$$

and so $h^{-1}k \in \bar{e}$. Hence $\bar{e} \leqslant G$. Finally if $h \in \bar{e}$ and $g \in G$ then

$$g^{-1}hg \sim g^{-1}g = e$$

and so $g^{-1}hg \in \bar{e}$ and $\bar{e} \lhd G$.

(b) $G/\sim$ is naturally isomorphic to $G/\bar{e}$ via the isomorphism

$$\phi\colon G/\sim \to G/\bar{e}, \qquad \phi(\bar{g}) = g\bar{e}.$$

Firstly this is well-defined: for if $\bar{g} = \bar{h}$ then $h^{-1} \sim g^{-1}$ and so $h^{-1}g \sim g^{-1}g = e$. Then $h^{-1}g \in \bar{e}$ and $g\bar{e} = h\bar{e}$. Finally

$$\phi(\bar{g}\,\bar{h}) = \phi(\overline{gh}) = (gh)\bar{e} = (g\bar{e})\,(h\bar{e}) = \phi(\bar{g})\phi(\bar{h}).$$

■

8. FIRST ISOMORPHISM THEOREM

The usefulness of quotient groups will become more apparent once we understand the implications of the *First Isomorphism Theorem.* This theorem will have particular importance in answering the question: find all the homomorphisms between two groups G and H. This is relatively straightforward when G is cyclic.

Proposition 231 *The map $\phi\colon \mathbb{Z}_m \to \mathbb{Z}_n$ given by*

$$\phi(r \bmod m) = kr \bmod n$$

is a well-defined homomorphism if and only if n divides km. As $\mathbb{Z}_m$ is cyclic then every homomorphism $\mathbb{Z}_m \to \mathbb{Z}_n$ is of this form.

Proof. If ϕ is a well-defined function then as $\bar{0} = \bar{m}$ in $\mathbb{Z}_m$ we need $\bar{0} = \overline{km}$ to be true in $\mathbb{Z}_n$. That is we need n to divide km. Conversely, suppose that n divides km so that $km = nc$ for some c. For ϕ to be well-defined, we need to ensure that

$$r_1 \bmod m = r_2 \bmod m \implies kr_1 \bmod n = kr_2 \bmod n,$$

or equivalently that if m divides $x = r_1 - r_2$ then n divides kx. If m divides x then $x = md$ for some d and hence

$$kx = k\,(md) = (km)\,d = (nc)\,d$$

is a multiple of n as required. It is then an easy check to see that $\phi(\bar{r}) = k\bar{r}$ is a homomorphism provided it is well-defined. ■

Example 232 *How many homomorphisms are there (i) from $\mathbb{Z}_6$ to $\mathbb{Z}_{12}$ (ii) from $\mathbb{Z}_{12}$ to $\mathbb{Z}_7$? (iii) from $\mathbb{Z}_{10}$ to D_8?*

Solution. (i) By the previous proposition we know that any homomorphism $\mathbb{Z}_6 \to \mathbb{Z}_{12}$ is of the form $\bar{r} \mapsto k\bar{r}$ where $12|6k$ or equivalently $2|k$. Hence k is even. But as k and $k+12$ would lead to the same homomorphism then there are in fact only six homomorphisms

$$\bar{n} \mapsto 0, \qquad \bar{n} \mapsto 2\bar{n}, \qquad \bar{n} \mapsto 4\bar{n}, \qquad \bar{n} \mapsto 6\bar{n}, \qquad \bar{n} \mapsto 8\bar{n}, \qquad \bar{n} \mapsto 10\bar{n}.$$

(ii) Homomorphisms $\mathbb{Z}_{10} \to D_8$. As in Proposition 188, it again follows that ϕ is entirely determined by $\phi(1)$ as $\mathbb{Z}_{10}$ is cyclic. Further $\mathrm{o}(1) = 10$ and so $\mathrm{o}(\phi(1))$ divides 10. Also $\mathrm{o}(\phi(1))$ divides $|D_8| = 8$ as a consequence of Lagrange's Theorem. Combining these facts we see $\mathrm{o}(\phi(1))$ divides 2. The orders of the elements of D_8 are given in the table below:

g	e	r	r^2	r^3	s	rs	r^2s	r^3s
$\mathrm{o}(g)$	1	4	2	4	2	2	2	2

The possible values of $\phi(1)$ are $e, r^2, s, rs, r^2s, r^3s$ and again each of these leads to a well-defined homomorphism.

$$\bar{n} \mapsto e, \qquad \bar{n} \mapsto r^{2n}, \qquad \bar{n} \mapsto s^n, \qquad \bar{n} \mapsto (rs)^n, \qquad \bar{n} \mapsto \left(r^2s\right)^n, \qquad \bar{n} \mapsto \left(r^3s\right)^n.$$

■

Example 233 *Find the kernels and images of the homomorphisms in Example 232.*

Solution. (i).Homomorphisms from $\mathbb{Z}_6$ to $\mathbb{Z}_{12}$.

ϕ	$\bar{n} \mapsto 0$	$\bar{n} \mapsto 2\bar{n}$	$\bar{n} \mapsto 4\bar{n}$	$\bar{n} \mapsto 6\bar{n}$	$\bar{n} \mapsto 8\bar{n}$	$\bar{n} \mapsto 10\bar{n}$
$\ker\phi$	$\mathbb{Z}_6$	$\{\bar{0}\}$	$\{\bar{0}, 3\}$	$\{\bar{0}, \bar{2}, \bar{4}\}$	$\{\bar{0}, \bar{3}\}$	$\{\bar{0}\}$
$\operatorname{Im}\phi$	$\{\bar{0}\}$	$\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$	$\{\bar{0}, \bar{4}, \bar{8}\}$	$\{\bar{0}, \bar{6}\}$	$\{\bar{0}, \bar{4}, \bar{8}\}$	$\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$

Note in each case that $|\ker\phi| \times |\operatorname{Im}\phi| = 6 = |\mathbb{Z}_6|$.

(ii) Homomorphisms from $\mathbb{Z}_{10}$ to D_8.

ϕ	$\bar{n} \mapsto e$	$\bar{n} \mapsto r^{2n}$	$\bar{n} \mapsto s^n$	$\bar{n} \mapsto (rs)^n$	$\bar{n} \mapsto (r^2s)^n$	$\bar{n} \mapsto (r^3s)^n$
$\ker\phi$	$\mathbb{Z}_6$	$\langle\bar{2}\rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$	$\langle\bar{2}\rangle$	$\langle\bar{2}\rangle$	$\langle\bar{2}\rangle$	$\langle\bar{2}\rangle$
$\operatorname{Im}\phi$	$\{e\}$	$\{e, r\}$	$\{e, s\}$	$\{e, rs\}$	$\{e, r^2s\}$	$\{e, r^3s\}$

Notice in each case that $|\ker\phi| \times |\operatorname{Im}\phi| = 10 = |\mathbb{Z}_{10}|$. ■

Let G be a group and consider finding all the homomorphisms from $\mathbb{Z}$ to G. A particular homomorphism ϕ is entirely determined by $\phi(1)$. If $g = \phi(1)$ and $n = o(g) < \infty$ then we see that $\operatorname{Im}\phi = \langle g\rangle \cong \mathbb{Z}_n$ and that $\ker\phi = n\mathbb{Z}$. We have wrapped $\mathbb{Z}$ into G going around and around $\langle g\rangle$ and repeating with period n. The map ϕ is not 1-1 and we have collapsed its domain, $\mathbb{Z}$, in such a way for its image to match a subgroup of G. More technically we have that $G/\ker\phi = \mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\operatorname{Im}\phi \cong \mathbb{Z}_n$ with the pre-image of any element of the image being a coset of the kernel.

If we are considering homomorphisms from $\mathbb{Z}_m$ into G these are likewise determined by $\phi(\bar{1})$ as $\mathbb{Z}_m$ is cyclic but we can only have $\phi(\bar{1}) = g$ if $o(g) = n$ divides m as we must have that $\phi(\bar{m}) = e_G$ for well-definedness. In this case $\ker\phi = \langle\bar{n}\rangle$ and again we are collapsing $\mathbb{Z}_m$ onto $\mathbb{Z}_m/\langle\bar{n}\rangle \cong \mathbb{Z}_n \cong \langle g\rangle$.

More generally, when considering homomorphisms $\phi\colon G \to H$ where G need not be cyclic, we will still be addressing the same problem of how are we to collapse the group G by $\ker\phi$ in order to fit G onto some subgroup of H as its image. This is where the First Isomorphism Theorem helps.

Theorem 234 *(**First Isomorphism Theorem**, Jordan 1870) Let $\phi\colon G \to H$ be a homomorphism between two groups. Then*

(a) $\ker\phi \lhd G$;

(b) $\operatorname{Im}\phi \leqslant H$;

(c) the map $g\ker\phi \mapsto \phi(g)$ gives an isomorphism

$$\frac{G}{\ker\phi} \cong \operatorname{Im}\phi.$$

Corollary 235 *Let $\phi\colon G \to H$ be a homomorphism between two groups and assume G is finite. Then*

$$|G| = |\ker\phi| \times |\operatorname{Im}\phi|$$

Proof. Parts (a) and (b) have been proven already in Propositions 192 and 193.

(c) Consider the map

$$\bar{\phi}\colon \frac{G}{\ker\phi} \to \operatorname{Im}\phi \qquad \text{given by} \qquad g\ker\phi \mapsto \phi\left(g\right).$$

Let $g_1, g_2 \in G$. From Proposition 199

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

This both shows that $\bar{\phi}$ is well-defined and that $\bar{\phi}$ is 1-1. It is also clear that $\bar{\phi}$ is onto. Finally $\bar{\phi}$ is a homomorphism as

$$\bar{\phi}((g_1\ker\phi) * (g_2\ker\phi)) = \bar{\phi}((g_1g_2)\ker\phi) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \bar{\phi}(g_1\ker\phi) * \bar{\phi}(g_2\ker\phi).$$

The Corollary follows because the order of $G/\ker\phi$ is $|G| / |\ker\phi|$ by Lagrange's Theorem ■

Example 236 *For* sgn: $S_n \to \{\pm1\}$, *the Isomorphism Theorem reads* $S_n/A_n \cong \{\pm1\}$.

Example 237 *For* det: $GL(n,\mathbb{R}) \to \mathbb{R}^*$, *the Isomorphism Theorem reads*

$$GL(n,\mathbb{R})/SL(n,\mathbb{R}) \cong \mathbb{R}^*.$$

Example 238 *For projection onto the first coordinate* $\pi_1\colon G_1 \times G_2 \to G_1$, *the Isomorphism Theorem reads* $(G_1 \times G_2) / (\{e\} \times G_2) \cong G_1$.

Example 239 *For* $\phi\colon \mathbb{Z} \to \mathbb{Z}$ *given by* $\phi(x) = nx$, *then the Isomorphism Theorem reads* $\mathbb{Z} = \mathbb{Z}/\{0\} \cong n\mathbb{Z}$.

Example 240 *For* $\phi\colon \mathbb{Z} \to \mathbb{Z}_n$ *given by* $\phi\left(x\right) = \bar{x}$, *then the Isomorphism Theorem reads* $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Example 241 *For* $\phi\colon \mathbb{Z}_8 \to \mathbb{Z}_{12}$ *given by* $\phi\left(\bar{x}\right) = 3\bar{x}$ *then the Isomorphism Theorem reads* $\mathbb{Z}_8/\langle\bar{4}\rangle \cong \langle\bar{3}\rangle$.

Example 242 *And for the following abelian groups, applying the Isomorphism Theorem to the homomorphism* $\phi(x) = x^2$ *gives*

$$S^1/\{\pm1\} \cong S^1, \qquad \mathbb{Z}_5/\{\bar{0}\} \cong \mathbb{Z}_5, \qquad \mathbb{Z}_6/\langle\bar{3}\rangle \cong \langle\bar{2}\rangle.$$

Remark 243 *The question of finding how many homomorphisms* $\phi\colon G \to H$ *there are between two groups* G *and* H *can be a difficult one if the groups are large and internally complicated, but the Isomorphism Theorem gives us a means in principle to determine that number. The process is as follows:*
(i) Determine the normal subgroups N *of* G. *(These are the potential kernels.)*
(ii) Determine the number of subgroups in H *which are isomorphic to* G/N; *let's call this number* $n(N)$. *(These are the possible images when the kernel is* N.*)*
(iii) For those normal subgroups where $n(N) > 0$, *determine the order of* $\operatorname{Aut}(G/N)$.

Then the number of homomorphisms from G to H is

$$\sum_{n(N)>0} n(N) \times |\mathrm{Aut}(G/N)|\,.$$

To explain this formula, the Isomorphism Theorem tells us that any homomorphism will map G onto an image which is isomorphic to G/N for some normal subgroup N. Conversely, given a subgroup $I \leqslant H$ which is isomorphic to G/N for some normal N, there are $|\mathrm{Aut}(G/N)|$ isomorphisms ι from G/N to I and for each such isomorphism the map

$$G \xrightarrow{\pi} G/N \xrightarrow{\iota} I$$

*(where $\pi\colon G \to G/N$ is the map $g \mapsto gN$) will be a homomorphism from G to H with image I. This is a **very** general approach to the problem at hand. In the case of G being cyclic or small, it may well be **much easier** to focus on some generators of G and consider their possible images, recalling that $\mathrm{o}(\phi(g))$ divides $\mathrm{o}(g)$ as we did in Example 233. Approaching it that way though, you will of course need to make sure that **potential** $\phi(g)$ do indeed lead to **actual** homomorphisms.*

Example 244 *How many homomorphisms are there from S_3 to $C_4 \times C_2$?*

Solution. Take g and h to be generators, respectively, of C_4 and C_2.

Recall that the normal subgroups of S_3 are $\{e\}, A_3, S_3$ (see Example 210) and we have that

$$S_3/\{e\} \cong S_3, \qquad S_3/A_3 \cong C_2, \qquad S_3/S_3 \cong \{e\}\,.$$

There are no homomorphisms with kernel $\{e\}$ as $C_4 \times C_2$ has no subgroup isomorphic to S_3 (which is not abelian).

There are 3 elements in $C_4 \times C_2$ with order 2, namely $(e,h), (g^2,h), (g^2,e)$ and to each of these corresponds a homomorphism with kernel A_3.

The final homomorphism is the map $\phi(\sigma) = (e,e)$ for all $\sigma \in S_3$. In all, then, there are four such homomorphisms.

$$\phi_1(\sigma) = \begin{cases} (e,e) & \sigma \in A_3 \\ (\bar{0},h) & \sigma \notin A_3 \end{cases}, \quad \phi_2(\sigma) = \begin{cases} (e,e) & \sigma \in A_3 \\ (g^2,h) & \sigma \notin A_3 \end{cases}, \quad \phi_3(\sigma) = \begin{cases} (e,e) & \sigma \in A_3 \\ (g^2,3) & \sigma \notin A_3 \end{cases},$$

and $\phi_4(\sigma) = (e,e)$ for all σ. ■

Example 245 *How many homomorphisms are there from A_4 to S_3?*

Solution. We have seen (Example 86) that the conjugacy classes of A_4 are $\{e\}$ and

$$\{(12)(34),(13)(24),(14)(23)\}, \quad \{(123),(134),(214),(324)\}, \quad \{(132),(143),(124),(234)\}.$$

So the normal subgroups of A_4 are $\{e\}, V_4, A_4$ and we have that

$$A_4/\{e\} \cong A_4, \qquad A_4/V_4 \cong C_3, \qquad A_4/A_4 = \{e\}\,.$$

There is no subgroup of S_3 which is isomorphic to A_4 and one, namely A_3, which is isomorphic to C_3.

There is obviously one homomorphism with kernel A_4. And having $\ker\phi = V_4$ means that $\operatorname{Im}\phi$ is isomorphic to C_3 and so must be $A_3 \subseteq S_3$. However there are two isomorphisms from C_3 to C_3 and so two different ways of wrapping A_4/V_4 onto A_3 and hence two different homomorphisms $A_4 \to S_3$ with image A_3. Thus in all we have three homomorphisms $A_4 \to S_3$ given by

$$\phi_1(\sigma) = \begin{cases} e & \sigma \in V_4 \\ (123) & \sigma \in (123)\, V_4 \\ (132) & \sigma \in (132)\, V_4 \end{cases}, \qquad \phi_2(\sigma) = \begin{cases} e & \sigma \in V_4 \\ (132) & \sigma \in (123)\, V_4 \\ (123) & \sigma \in (132)\, V_4 \end{cases}, \qquad \phi_3(\sigma) = e.$$

■

Example 246 *Show that* $\operatorname{Aut}(V_4)$ *is isomorphic to* S_3.

Solution. If we write $a = (12)\,(34)\,,\ b = (13)\,(24)\,,\ c = (14)\,(23)$ then any automorphism of V_4 must send e to e and $\{a,b,c\}$ to $\{a,b,c\}$. Hence there are at most 6 automorphisms. However if we note V_4 may be presented as

$$\langle a,b\colon a^2 = e = b^2, ab = ba\rangle = \langle b,c\colon c^2 = e = b^2, bc = cb\rangle = \langle a,c\colon a^2 = e = c^2,\ ac = ca\rangle$$

then we see that there is a symmetry in the roles of a,b,c and so any element of $\operatorname{Sym}\{a,b,c\}$ is indeed an automorphism of V_4. ■

Example 247 *How many homomorphisms are there from* D_8 *to* A_4*?*

Solution. Recall that the conjugacy classes of D_8 are

$$\{e\}\,, \qquad \left\{r, r^3\right\}, \qquad \left\{r^2\right\}, \qquad \left\{s, r^2 s\right\}, \qquad \left\{rs, r^3 s\right\}.$$

Hence the normal subgroups of D_8 are

$$\begin{aligned} N_1 &= \{e\}\,, \qquad N_2 = \left\{e, r^2\right\}, \qquad N_3 = \left\{e, r, r^2, r^3\right\}, \\ N_4 &= \left\{e, s, r^2, r^2 s\right\}, \qquad N_5 = \left\{e, s, r^2, r^2 s\right\}, \qquad N_6 = D_8 \end{aligned}$$

and we have that (see Example 226)

$$D_8/N_1 \cong D_8, \qquad D_8/N_2 \cong V_4, \qquad D_8/N_3 \cong D_8/N_4 \cong D_8/N_5 \cong C_2, \qquad D_8/N_6 \cong \{e\}\,.$$

By Lagrange's Theorem, there is no subgroup of A_4 which is isomorphic to D_8. There is one subgroup (namely V_4) which is isomorphic to V_4 and three subgroups of A_4 which are isomorphic to C_2 (namely $\langle a\rangle, \langle b\rangle$ and $\langle c\rangle$).

From the previous example we know there are 6 homomorphisms with kernel N_2 and image V_4; such an example is

$$\phi(e) = \phi(r^2) = e, \quad \phi(r) = \phi(r^3) = a,, \quad \phi(s) = \phi(r^2 s) = b, \quad \phi(rs) = \phi(r^3 s) = c.$$

There are $3 \times 3 = 9$ homomorphisms with kernel N_3 or N_4 or N_5 and image $\langle a\rangle$ or $\langle b\rangle$ or $\langle c\rangle$; such an example is

$$\phi(e) = \phi(s) = \phi(r^2 s) = \phi(r^2) = e, \qquad \phi(r) = \phi(r^3) = \phi(rs) = \phi(r^3 s) = b.$$

Finally there is the homomorphism with image $\{e\}$.

In all then there are $6 + 9 + 1 = 16$ homomorphisms from D_8 to A_4. ■

9. GROUP ACTIONS

We move now, from thinking of groups in their own right, to thinking of how groups can move sets around – for example, how S_n permutes $\{1, 2, \ldots, n\}$ and matrix groups move vectors.

Definition 248 *A* ***left action of a group*** *G on a set S is a map*

$$\rho\colon G \times S \to S$$

such that:
(i) $\rho(e, s) = s$ for all $s \in S$;
(ii)$\rho(g, \rho(h, s)) = \rho(gh, s)$ for all $s \in S$ and $g, h \in G$.

Notation 249 *We will normally write $g \cdot s$ for $\rho(g, s)$ and so (i) and (ii) above would now read as:*
(i') $e \cdot s = s$ for all $s \in S$;
(ii') $g \cdot (h \cdot s) = (gh) \cdot s$ for all $s \in S$ and $g, h \in G$.

Remark 250 *We will think of $g \cdot s \in S$ as the point that s is moved to by g.*

Example 251 *The group $GL(n, \mathbb{R})$ acts on $\mathbb{R}^n$ by*

$$A \cdot \mathbf{v} = A\mathbf{v} \quad \textit{for} \quad A \in GL(n, \mathbb{R}) \ \textit{and}\ \mathbf{v} \in \mathbb{R}^n$$

as

$$I_n\mathbf{v} = \mathbf{v} \quad \textit{and} \quad (AB)\,\mathbf{v} = A\,(B\mathbf{v}) \quad \textit{for}\ \mathbf{v} \in \mathbb{R}^n,\ A, B \in GL(n, \mathbb{R}).$$

Example 252 *The group $GL(n, \mathbb{R})$ acts on the set $M_{nn}(\mathbb{R})$ of real $n \times n$ matrices by conjugation*

$$A \cdot M = AMA^{-1}.$$

We can verify that this is a left action by noting

$$I_n \cdot M = I_n M\, I_n^{-1} = M \quad \textit{and} \quad (AB) \cdot M = (AB)\, M\, (AB)^{-1} = A\left(BMB^{-1}\right) A^{-1} = A \cdot (B \cdot M)\,.$$

Example 253 *Another action of $GL(n, \mathbb{R})$ on the set $M_{nn}(\mathbb{R})$ is given by*

$$A \cdot M = AM.$$

Example 254 *Let S be a polygon in $\mathbb{R}^2$ or a polyhedron in $\mathbb{R}^3$. Then the symmetry group of S – those isometries g that satisfy $g(S) = S$ – acts naturally on S. The symmetry group can separately be considered as acting on the set of vertices of the polyhedron, or edges, or faces.*

Example 255 *Let S denote the set of triangles in $\mathbb{R}^2$ and let*

$$\begin{aligned} G_1 &= \left\{ \mathbf{v} \mapsto A\mathbf{v} + \mathbf{b} \colon\ A \in GL(2,\mathbb{R}),\ \mathbf{b} \in \mathbb{R}^2 \right\}. \\ G_2 &= \left\{ \mathbf{v} \mapsto A\mathbf{v} + \mathbf{b} \colon\ A \in O(2),\ \mathbf{b} \in \mathbb{R}^2 \right\}. \end{aligned}$$

That is, G_1 is the group of affine transformations of the plane and G_2 is the group of isometries of the plane. Then G_1 and G_2 act naturally on S by $g \cdot \Delta = g(\Delta)$.

And then there are various examples where a group acts on itself or subsets of itself in a natural way.

Example 256 *Let G be a group. Then we have a left action of G on itself by $g \cdot h = gh$ for $g, h \in G$.*

Example 257 *Let G be a group. Then we have a left action of G on itself by conjugation – that is*

$$g \cdot h = ghg^{-1}.$$

We clearly have $e \cdot g = g$ and

$$g \cdot (k \cdot h) = g \cdot \left(khk^{-1}\right) = gkhk^{-1}g^{-1} = (gk)\, h\, (gk)^{-1} = (gk) \cdot h.$$

Example 258 *Let H be a (not necessarily normal) subgroup of a group G and let G/H denote the set of left cosets of H. Then there is a left action of G on G/H by*

$$g_1 \cdot (g_2 H) = (g_1 g_2)\, H.$$

We can similarly consider *right actions* of groups:

Definition 259 *A* ***right action of a group*** *G on a set S is a map*

$$\rho \colon S \times G \to S$$

such that:
(i) $\rho(s, e) = s$ for all $s \in S$;
(ii) $\rho(\rho(s, h), g) = \rho(s, hg)$ for all $s \in S$ and $g, h \in G$.

There is no particular benefit to considering left actions over right actions or vice versa. Examples of right actions that we have met are:

Example 260 *(i) S_n acts on $\{1, 2, \ldots, n\}$ by $\rho(k, \sigma) = k\sigma$.*
(ii) S_n acts on the power set of $\{1, 2, \ldots, n\}$ (the set of subsets) by $\rho(S, \sigma) = S\sigma$.
(ii) $GL(n, \mathbb{R})$ acts on the set of $1 \times n$ row vectors by $\rho(\mathbf{v}, A) = \mathbf{v}A$.
(iii) A group G acts on the set of right cosets of a subgroup H by $\rho(Hk, g) = Hkg$.
(iv) A group G acts on itself by translation by $\rho(h, g) = hg$.
(v) A group G acts on itself by conjugation by $\rho(h, g) = g^{-1}hg$.

Definition 261 *If a group G acts on a set S and $s \in S$ then:*
(i) the ***orbit*** *of s, written $\operatorname{Orb}(s)$, is defined as*

$$\operatorname{Orb}(s) = \{g \cdot s \colon g \in G\} \subseteq S.$$

If there is only one orbit then we say that the action is ***transitive****.*
(ii) the stabilizer of s, written $\operatorname{Stab}(s)$, is defined as

$$\operatorname{Stab}(s) = \{g \in G \colon g \cdot s = s\} \subseteq G.$$

Example 262 *When S_n (right) acts on $\{1, 2, \ldots, n\}$ by $\rho(k, \sigma) = k\sigma$ then there is just one orbit. Note that*

$$\operatorname{Stab}(n) = \{\sigma \in S_n \colon n\sigma = n\} = \operatorname{Sym}\{1, 2, \ldots, n-1\} \cong S_{n-1}.$$

Example 263 *When S_n (right) acts on the subsets of $\{1, 2, \ldots, n\}$ by $\rho(S, \sigma) = S\sigma$ then there are $n + 1$ orbits, one for each possible size of $|S|$ and if $|S| = k$ then*

$$\operatorname{Stab}(S) \cong S_k \times S_{n-k}.$$

(See Exercise Sheet 6, Question 3.)

Example 264 *When $GL(n, \mathbb{R})$ acts on $\mathbb{R}^n$ by $A \cdot \mathbf{v} = A\mathbf{v}$, there are just two orbits $\{\mathbf{0}\}$ and $\mathbb{R}^n \backslash \{\mathbf{0}\}$. If $A \in GL(n, \mathbb{R})$ then $A\mathbf{0} = \mathbf{0}$ whilst if $\mathbf{v} \neq \mathbf{0}$ then $\mathbf{v}$ can be extended to a basis which can be used as the columns of an invertible matrix A. Then $A\mathbf{e}_1 = \mathbf{v}$ where $\mathbf{e}_1 = (1, 0, \ldots, 0)^T$.*

Example 265 *When $GL(2, \mathbb{C})$ acts on the set $M_{22}(\mathbb{C})$ of complex $n \times n$ matrices by conjugation*

$$A \cdot M = AMA^{-1},$$

then the an orbit either has a representative of the form

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \qquad \lambda, \mu \in \mathbb{C}$$

when the matrix is diagonalizable or of the form

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \qquad \lambda \in \mathbb{C}$$

when the matrix is not diagonalizable.

Example 266 *Let S be the set of black-or-white colourings of a square's edges. As there are four edges then $|S| = 2^4 = 16$. The square's symmetry group D_8 acts naturally on S and there are six orbits with a representative of each orbit listed below*

$$WWWW, \qquad BWWW, \qquad BBWW, \qquad BWBW, \qquad BBBW, \qquad BBBB,$$

where the edges' colours are listed in clockwise order.

Example 267 *Let S be the set of black-or-white colourings of a cube's faces. As there are six faces then $|S| = 2^6 = 64$. The cube's rotational symmetry group acts naturally on S and there are 10 orbits with a representative of each orbit listed below:*

all white,   1 black,   2 opposite black faces,   2 adjacent black faces,
3 black faces in a C,   3 black faces around a corner,
2 opposite white faces,   2 adjacent white faces,   1 white,   all black.

Example 268 *(From Example 255.) When the affine group group of $\mathbb{R}^2$ acts on the set of triangles, then there is just one orbit as any triangle can be taken to any other triangle via an affine map. The orbits when the isometry group acts are the congruence classes, as two triangle are related by an isometry if and only if they are congruent.*

Example 269 *When a group G acts on itself by $g \cdot h = gh$ then the action is transitive and each stabilizer is just $\{e\}$.*

Example 270 *When a group G acts on itself by $g \cdot h = ghg^{-1}$ then the orbit of g is its conjugacy class and its stabilizer is the centralizer $C_G(g)$.*

Example 271 *When $H \leqslant G$ and G acts on the set of cosets G/H by $g_1 \cdot (g_2 H) = (g_1 g_2) H$ then the action is transitive and the stabilizer of gH is gHg^{-1} as*

$$k \cdot gH = gH \iff kgH = gH \iff g^{-1}kg \in H \iff k \in gHg^{-1}.$$

We conclude with three important results relating to orbits and stabilizers.

Proposition 272 *The orbits of an action partition the set.*

Proof. Let G be a group acting on a set S. We introduce a binary relation $\sim$ on S by setting, for $s, t \in S$,

$$s \sim t \iff \text{there exists } g \in G \text{ such that } g \cdot s = t.$$

We shall show that $\sim$ is an equivalence relation and that the equivalence classes are the orbits.

(a) $\sim$ is reflexive as $s = e \cdot s$ for all $s \in S$;

(b) $\sim$ is symmetric as

$$\begin{aligned} s \sim t &\implies g \cdot s = t \text{ for some } g \in G \\ &\implies g^{-1} \cdot t = s \\ &\implies t \sim s. \end{aligned}$$

(c) $\sim$ is transitive as

$$\begin{aligned} s \sim t,\, t \sim u &\implies g \cdot s = t \text{ and } h \cdot t = u \text{ for some } g, h \in G \\ &\implies (hg) \cdot s = h \cdot (g \cdot s) = h \cdot t = u \\ &\implies s \sim u. \end{aligned}$$

Hence $\sim$ is an equivalence relation and, in particular, the equivalence classes partition S. For $s \in S$, note that the equivalence class $\bar{s}$ equals

$$\bar{s} = \{g \cdot s \colon g \in G\} = \operatorname{Orb}(s).$$

■

Proposition 273 *The stabilizers of an action are subgroups.*

Proof. Let G be a group acting on a set S and $s \in S$. Then

$$e \in \mathrm{Stab}(s) \quad \text{as} \quad e \cdot s = s.$$

If $g, h \in \mathrm{Stab}(s)$ then

$$(gh) \cdot s = g \cdot (h \cdot s) = g \cdot s = s$$

showing that $gh \in \mathrm{Stab}(s)$ and

$$g^{-1} \cdot s = g^{-1} \cdot (g \cdot s) = \left(g^{-1}g\right) \cdot s = e \cdot s = s$$

showing that $g^{-1} \in \mathrm{Stab}(s)$. ■

Proposition 274 *If two elements lie in the same orbit then their stabilizers are conjugate.*

Proof. If s, t lie in the same orbit of an action then there exists $g \in G$ such that $g \cdot s = t$. Then

$$\begin{aligned} h \in \mathrm{Stab}(s) &\iff h \cdot s = s \\ &\iff h \cdot \left(g^{-1} \cdot t\right) = g^{-1} \cdot t \\ &\iff g \cdot \left(h \cdot \left(g^{-1} \cdot t\right)\right) = g^{-1} \cdot t = t \\ &\iff \left(ghg^{-1}\right) \cdot t = t \\ &\iff ghg^{-1} \in \mathrm{Stab}(t) \\ &\iff h \in g^{-1}\mathrm{Stab}(t)g. \end{aligned}$$

Hence

$$\mathrm{Stab}(s) = g^{-1}\mathrm{Stab}(t)g.$$

■

10. ORBIT-STABILIZER THEOREM

Theorem 275 ***(Orbit-Stabilizer Theorem)*** *Let G be a finite group acting on a set S and let $s \in S$. Then*

$$|G| = |\mathrm{Stab}(s)| \times |\mathrm{Orb}(s)|\,.$$

Proof. We shall show that there is a well-defined bijection between the cosets of $\mathrm{Stab}(s)$ in G and $\mathrm{Orb}(s)$. This will then mean by Lagrange's Theorem that

$$\frac{|G|}{|\mathrm{Stab}(s)|} = \#\text{ cosets of } \mathrm{Stab}(s) = |\mathrm{Orb}(s)|\,.$$

We define the map

$$\phi\colon G/\mathrm{Stab}(s) \to \mathrm{Orb}(s) \qquad \text{by} \qquad \phi(g\mathrm{Stab}(s)) = g \cdot s.$$

We first need to show that ϕ is well-defined (i.e. that the image of the coset $g\mathrm{Stab}(s)$ is not dependent on the choice of representative g). Note that

$$\begin{aligned} g\mathrm{Stab}(s) = h\mathrm{Stab}(s) \iff & \quad h^{-1}g \in \mathrm{Stab}(s) \\ \iff & \quad h^{-1}g \cdot s = s \\ \iff & \quad g \cdot s = h \cdot s. \end{aligned}$$

This shows that ϕ is indeed well-defined. The reverse implications show that ϕ is 1–1. Finally it is immediately apparent that ϕ is onto as every element of $\mathrm{Orb}(s)$ can be written as $g \cdot s$ for some g. ■

Remark 276 *In fact, ϕ is more than just a bijection, it is an isomorphism of actions of G. If G acts on two sets S and T, an isomorphism of these actions is a bijection $\phi\colon S \to T$ such that*

$$\phi(g \cdot s) = g \cdot (\phi(s)).$$

Remark 277 *As an immediate consequence, note that the size of an orbit must divide the order of the group. (We already knew this to be true of stabilizers as they are subgroups.)*

Corollary 278 *(Lagrange's Theorem) Let G be a group and $H \leqslant G$. Then G acts on G/H by*

$$g \cdot (kH) = (gk)\,H.$$

Proof. With this action

$$\mathrm{Stab}(H) = H \qquad \text{and} \qquad \mathrm{Orb}(H) = G/H.$$

By the Orbit-Stabilizer Theorem

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

■

Corollary 279 *Let G be a group, $g \in G$ and*

$$\begin{aligned} C_G(g) &= \{h \in G \colon gh = hg\} = \textit{ centralizer of } g, \\ C(g) &= \left\{h^{-1}gh \colon h \in G\right\} = \textit{ conjugacy class of } g. \end{aligned}$$

Then

$$|C_G(g)| \times |C(g)| = |G|.$$

Proof. G acts on itself by conjugation:

$$g \cdot h = ghg^{-1}.$$

For $g \in G$

$$\operatorname{Stab}(g) = \left\{h \in G \colon hgh^{-1} = g\right\} = C_G(g), \qquad \operatorname{Orb}(g) = C(g).$$

■

Example 280 *Determine the number of conjugates of* $(1\,2\,3)$ *in* A_5*.*

Solution. First we will find $C_{A_5}((123))$. We note

$$(123)\,\rho = \rho\,(123) \iff (123) = \rho^{-1}\,(123)\,\rho = (1\rho\,2\rho\,3\rho)\,.$$

As there are three ways of writing (123), the others being (231) and (312), then

$$1\rho = 1,\ 2\rho = 2,\ 3\rho = 3 \quad \text{or} \quad 1\rho = 2,\ 2\rho = 3,\ 3\rho = 1 \quad \text{or} \quad 1\rho = 3,\ 2\rho = 1,\ 3\rho = 2.$$

So $1, 2, 3$ must cycle in one of three ways, all of them even permutations. For ρ to be even, it must be the case that $4\rho = 4$ and $5\rho = 5$. Hence $|C_{A_5}((123))| = 3$ and

$$|C\,((123))| = \frac{|A_5|}{3} = \frac{60}{3} = 20.$$

As there are, in all, $\frac{5\times4\times3}{3} = 20$ 3-cycles in A_5 then the conjugacy class of (123) in A_5 is the entire set of 3-cycles. (Compare this with Example 86.) ■

Example 281 *Show that there are* 12 *rotational symmetries of a regular tetrahedron and* 24 *of a cube.*

Solution. Let G_T denote the tetrahedral group. A tetrahedron has 4 vertices and G_T acts transitively on this set. The stabilizer of a particular vertex v consists of the identity and the two $\pm 120°$ rotations about an axis through v and the midpoint of the opposite face. Hence

$$|G_T| = |\operatorname{Stab}(v)| \times |\operatorname{Orb}(v)| = 3 \times 4 = 12.$$

Let G_C denote the cube's group. A cube has 8 vertices and G_C acts transitively on this set. The stabilizer of a particular vertex v consists of the identity and the two $\pm 120°$ rotations about the diagonal through v and its opposite vertex. Hence

$$|G_C| = |\operatorname{Stab}(v)| \times |\operatorname{Orb}(v)| = 3 \times 8 = 24.$$

Either of these calculations could as easily have been performed by looking at the actions on edges and faces. Using the faces of a cube, for example, we would have concluded

$$|G_C| = |\operatorname{Stab}(f)| \times |\operatorname{Orb}(f)| = 4 \times 6 = 24.$$

■

Proposition 282 *A group G of order p^r, where p is prime, has a non-trivial centre.*

Proof. Let G act on itself by conjugation. Recall that the centre of G is $Z(G) = \{g \in G \colon hg = gh\ \forall h \in H\}$ so being in $Z(G)$ is equivalent to being a singleton orbit. There is at least one such orbit, namely $\{e\}$. By the Orbit-Stabilizer Theorem, all the orbits have size p^k for some $0 \leqslant k < r$. If N_k is the number of such orbits then, as the orbits partition G we have

$$N_0 + N_1 p + N_2 p^2 + \cdots + N_{r-1} p^{r-1} = p^r,$$

and in particular we see that N_0 is a multiple of p. As $N_0 \geqslant 1$ then there are other singleton orbits, i.e. other elements of $Z(G)$. ■

Proposition 283 *A group G of order p^2 is isomorphic to C_{p^2} or $C_p \times C_p$.*

Proof. If G has an element of order p^2 then $G \cong C_{p^2}$. If there is no such element, then the non-trivial elements have order p. Take a non-trivial element x from the centre $Z(G)$ and another element y not in $\langle x \rangle$. Then the elements $x^i y^j$ $(0 \leqslant i, j < p)$ are all distinct as $\langle x \rangle \cap \langle y \rangle = \{e\}$. Further as x is $Z(G)$ then these elements multiply by

$$x^i y^j * x^I y^J = x^{i+I} y^{j+J}$$

and we see that $G \cong C_p \times C_p$. ■

Example 284 *Let G be a group with three conjugacy classes. Show that $G \cong C_3$ or $G \cong S_3$.*

Solution. The conjugacy class of e is just $\{e\}$. Denote the size of the remaining two classes as c_1 and c_2. Both c_1 and c_2 are factors of $|G|$ and so $|G| = k_1 c_1 = k_2 c_2$ for some k_1, k_2. Without any loss of generality we may assume that $k_1 \leqslant k_2$. As the conjugacy classes partition G then

$$1 + c_1 + c_2 = k_1 c_1 = k_2 c_2$$

so that

$$1 + c_2 = (k_1 - 1) c_1, \qquad 1 + c_1 = (k_2 - 1) c_2.$$

Eliminating c_2 and rearranging somewhat, we arrive at

$$c_1 = \frac{k_2}{(k_1 - 1)(k_2 - 1) - 1}.$$

If $k_1 > 3$ then we have the contradiction

$$\frac{k_2}{(k_1 - 1)(k_2 - 1) - 1} < \frac{k_2}{2(k_2 - 1) - 1} = \frac{k_2}{2k_2 - 3} < 1.$$

If $k_1 = 1$ then $c_1 = -k_2 < 0$, a further contradiction. So the possibilities are

$$\begin{array}{rclllll} k_1 &=& 2, & k_2 = 3, & c_1 = 3, & c_2 = 2, & |G| = 6; \\ k_1 &=& 3, & k_2 = 3, & c_1 = 1, & c_2 = 1, & |G| = 3. \end{array}$$

As C_6 has six conjugacy classes, the first possibility leads to S_3 only and the second to C_3. ■

Theorem 285 ***(Cauchy's Theorem)*** *Let G be a finite group and let p be a prime dividing $|G|$. Then G has an element of order p.*

Proof. Let S denote the set

$$S = \{(g_1, g_2, \ldots, g_p) \in G^p \colon g_1 g_2 \cdots g_p = e\}.$$

Note that $|S| = |G|^{p-1}$ as the first $p-1$ elements $g_1, \ldots, g_{p-1}$ may be chosen freely from G and then $g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$ is determined. Let $\sigma = (123 \cdots p)$ and note that there is an action of $\langle \sigma \rangle \cong C_p$ on S by

$$\sigma \cdot (g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1)$$

as

$$\begin{aligned} (g_1, g_2, \ldots, g_p) \in S \iff & \quad g_1 g_2 \cdots g_p = e \\ \iff & \quad g_2 \cdots g_p = g_1^{-1} \\ \iff & \quad g_2 \cdots g_p g_1 = e \\ \iff & \quad (g_2, g_3, \ldots, g_p, g_1) \in S. \end{aligned}$$

We consider the orbits of this action. As $|\langle \sigma \rangle| = p$ then, by the Orbit-Stabilizer Theorem, the orbits may have size 1 or p. If $(g_1, g_2, \ldots, g_p)$ is in an orbit of size 1 then

$$\sigma \cdot (g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1) = (g_1, g_2, \ldots, g_p)$$

and hence we see that

$$g_1 = g_2 = \cdots = g_p \qquad \text{and} \qquad (g_1)^p = e.$$

We also see that there is at least one singleton orbit, namely $\{(e, e, \ldots, e)\}$. As the orbits partition S then

$$|S| = k + lp$$

where k is the number of singleton orbits and l is the number of orbits of size p. As p divides $|G|$ then p divides $|S| = |G|^{p-1}$ and hence p divides k. From our earlier comment $k \geqslant 1$ and hence there is at least one other singleton orbits besides $\{(e, e, \ldots, e)\}$. Again from our earlier comments, this other singleton orbit is of the form $\{(g, g, \ldots, g)\}$ where $g^p = e$. ■

11. COUNTING ORBITS

Theorem 286 ***(Orbit Counting Formula)*** *Let G be a finite group acting on a finite set S. Then*

$$\# \textit{ orbits} = \frac{1}{|G|}\sum_{g\in G}|\text{fix}(g)|$$

where, for $g \in G$, we define

$$\text{fix}(g) = |\{s \in S \colon g \cdot s = s\}| .$$

Proof. We will consider the set

$$A = \{(g,s) : g \cdot s = s\} \subseteq G \times S$$

and count up $|A|$ in two different ways. Then

$$|A| = \sum_{g\in G}|\{s \in S \colon g\cdot s = s\}| = \sum_{s \in S}|\{g \in G \colon g \cdot s = s\}| .$$

The first and second sums respectively equal

$$\sum_{g\in G}|\text{fix}(g)| \qquad \text{and} \qquad \sum_{s\in S}|\text{Stab}(s)| .$$

If the orbits are $O_1, O_2, \ldots, O_N$ then

$$\sum_{s\in S}|\text{Stab}(s)| = \sum_{i=1}^{N}\sum_{s\in O_i}|\text{Stab}(s)| \qquad \text{[as the orbits partition } S\text{]}.$$

Using the Orbit-Stabilizer Theorem, this is turn can be rewritten as

$$\sum_{i=1}^{N}\sum_{s\in O_i}|\text{Stab}(s)| = \sum_{i=1}^{N}\sum_{s\in O_i}\frac{|G|}{|O_i|} = \sum_{i=1}^{N}|G| = N\,|G| .$$

Hence

$$N\,|G| = \sum_{g\in G}|\text{fix}(g)|$$

and the result follows. ■

Remark 287 *Note that if g and h are conjugate then* $\text{fix}(g) = \text{fix}(h)$. *To see this, say $g = k^{-1}hk$, and note*

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

So we can rewrite the orbit counting formula as

$$N = \frac{1}{|G|}\sum_{g\in C_i}|\text{fix}(g)|\,|C(g)|$$

where we take a representative g from each of the conjugacy classes C_i.

Remark 288 *The orbit counting formula is often (incorrectly) called* ***Burnside's Lemma*** *as it was stated and proved in an 1897 text of William Burnside, but the result had been much earlier known to Frobenius and Cauchy.*

Example 289 *In how many essentially different ways can a triangle's edges be painted with* n *colours. Compare your answers for* $n = 2$ *and* $n = 3$ *with those found in Sheet 6, Exercise 4.*

Solution. With labels still present there are n^3 colourings. So we can form the table

g	# of conjugates	s fixed by g	fix(g)	contribution
e	1	all	n^3	n^3
r	2	$C_1C_1C_1$	n	$2n$
s	3	$C_1C_1C_2$	n^2	$3n^2$

By the orbit counting formula there are

$$\frac{n^3 + 3n^2 + 2n}{6} = \frac{n\,(n+1)\,(n+2)}{6}$$

essentially different colourings. Note this fomula gives $2 \times 3 \times 4/6 = 4$ and $3 \times 4 \times 5/6 = 10$ colourings when $n = 2$ and $n = 3$ as previously calculated. ∎

Remark 290 *How might this have been calculated directly? The triangles sides might be coloured with* 1 *or* 2 *or* 3 *colourings. There are respectively* n *and* $2\binom{n}{2}$ *and* $\binom{n}{3}$ *such colourings and so we again arrive at the answer*

$$n + \frac{2n\,(n-1)}{2} + \frac{n\,(n-1)\,(n-2)}{6} = \frac{6n + (6n^2 - 6n) + (n^3 - 3n^2 + 2n)}{6} = \frac{n^3 + 3n^2 + 2n}{6}.$$

However, once we move on to geometric objects with more symmetries, a direct approach quickly becomes intractable.

Example 291 *A cuboid has distinct dimensions. In how many (essentially different) ways can the cuboid's faces be painted black or white? Determine this number when two of the cuboid's dimensions are equal.*

Solution. As the cuboid's dimensions are distinct then its symmetry group is $C_2 \times C_2$ (like that of a rectangle). The three non-trivial elements are rotations through a half-turn about each of the x- y- and z-axes.

There are $2^6 = 64$ ways of colouring these faces whilst labelled. As the symmetry group is abelian, the conjugacy classes are singleton sets; however we can see that each of the non-trivial elements will fix the same number of colourings. Applying the orbit counting formula we arrive at the table

g	like elements	s fixed by g	fix(g)	contribution
e	1	all	64	64
$\neq e$	3	$C_1C_1C_2C_2C_3C_4$	16	48

Our answer is then

$$\frac{64 + 48}{4} = 16 + 12 = 28.$$

When two (but not three) of the dimensions are the same then the symmetry group is now D_8. Arguing similarly we arrive at the table

g	conjugates	s fixed by g	fix(g)	contribution
e	1	all	64	64
r	2	$C_1C_2C_2C_2C_2C_3$	8	16
r^2	1	$C_1C_2C_3C_2C_3C_4$	16	16
s	2	$C_1C_2C_3C_2C_4C_1$	16	32
rs	2	$C_1C_2C_2C_3C_3C_1$	8	16

Our answer is then

$$\frac{64+16+16+32+16}{8} = 8+2+2+4+2 = 18.$$

■

Example 292 *How many different triples (x_1, x_2, x_3) of positive integers are there such that $x_1 + x_2 + x_3 = 100$ and $x_1 \leqslant x_2 \leqslant x_3$.*

Proof. Let

$$S = \{(x_1, x_2, x_3) : x_i \geqslant 1,\ x_1 + x_2 + x_3 = 100\}.$$

Then S_3 acts naturally on S and in each orbit of this action there is a unique (x_1, x_2, x_3) such that $x_1 \leqslant x_2 \leqslant x_3$. So the question is equivalent to finding the number of orbits of this action. Note that x_1 can be any number from 1 to 98, and x_2 any number from 1 to $99 - x_1$, with x_3 then determined by the choices of x_1 and x_2. So

$$|S| = \sum_{x_1=1}^{98} (99 - x_1) = 99 \times 98 - \frac{1}{2} \times 98 \times 99 = 49 \times 99 = 4851.$$

We apply the orbit counting formula as below:

g	conjugates	s fixed by g	fix(g)	contribution
e	1	(x_1, x_2, x_3)	4851	4851
(12)	3	(x_1, x_1, x_3)	49	147
(123)	2	(x_1, x_1, x_1)	0	0

Hence the number of orbits (and our answer) equals

$$\frac{4851 + 147}{6} = 833.$$

■

Example 293 *How many essentially different ways are there to make a bracelet which has three red beads, two blue beads and two white beads?*

Proof. These seven beads can be considered to occupy the vertices of a regular heptagon and then two different colourings would be considered indistinguishable if some element of D_{14} connects the two. So we are again being asked to determine the number of orbits of this action of D_{14} on the set of (labelled) colourings.

The total number of different colourings (whilst the positions are labelled) is

$$\frac{7!}{3!2!2!} = \frac{5040}{6 \times 2 \times 2} = 210.$$

Let r denote a rotation by $2\pi/7$ and s denote a (fixed) reflection. Note that a rotation (in this case) would only fix those colourings that are monochromatic (not possible here). All reflections are in an axis that goes through a vertex and the opposite edge's midpoint. A colouring would be fixed if vertices and their mirror images were of the same colour; with the given beads this is only possible if we colour the vertex on the axis red and the other six in pairs opposite one another (one pair red, one blue, one white). There are $6 = 3!$ ways of doing this. Hence our answer is

$$\frac{\overbrace{210}^{e} + \overbrace{6 \times 0}^{\text{rotations}} + \overbrace{7 \times 3!}^{\text{reflections}}}{14} = \frac{210 + 42}{14} = 15 + 3 = 18.$$

■

Remark 294 *We can already see (though the answer is still relatively small) that it would be rather difficult to list these* 18 *arrangements by inspection and be confident we had not listed a colouring twice nor missed any colouring. The eighteen colourings are in fact*

$$\begin{array}{llllll} RRRWWBB & RRRBWWB & RRWRBBW & RRBRWWB & RRBWRWB & RBRBRWW \\ RRRWBBW & RRWRWBB & RRBRBWW & RRWWRBB & RRBWRBW & RBRWRBW \\ RRRWBWB & RRWRBWB & RRBRWBW & RRWBRBW & RWRWRBB & RBRWRWB \end{array}$$

Example 295 *Anticipating* 10 *students for his option, a tutor assigns* 5 *weekly slots in his diary. In the end only* 6 *students choose to take the option. The tutor allows them to choose from the available slots, stipulating only a maximum of* 2 *students per slot. In how many different ways can the students choose to arrange themselves?*

Solution. If there had been 10 students taking the option then the slots could have been distributed in

$$\frac{10!}{(2!)^5} = 113400$$

ways. With, instead, 6 students on the option then there will be 4 unused places. Different assignings of these places to the 4 "missing" students correspond to the same assignings of places to the 6 students – which is precisely the number of assignings we are seeking to calculate. So, alternatively, we can let S_4 act on the unoccupied places from the 113400 original assignings and determine the number of orbits of this action. For example, if we list the six students' slots first then the unoccupied ones, we see that 123441(2355) leads to the same teaching arrangements as 123441(5325).

g	conjugates	fixed by g	fix(g)	contribution
e	1	all	113400	113400
(12)	6	$S_1S_1S_2S_3$	12600	75600
(123)	8	$S_1S_1S_1S_2$	0	0
(1234)	6	$S_1S_1S_1S_1$	0	0
$(12)\,(34)$	3	$S_1S_1S_2S_2$	1800	5400

Note that, with up to two students allowed per slot, there are no arrangements of the form $S_1S_1S_1S_1$ or $S_1S_1S_1S_2$. Of the form $S_1S_1S_2S_2$ there are

$$\frac{6!}{0!0!2!2!2!}\times\underbrace{5\times4}_{\text{choice of }S_1\text{ and }S_2}=1800$$

arrangements fixed and of the form $S_1S_1S_2S_3$ (where S_2 and S_3 may be the same) there are

$$1800+\frac{6!}{0!1!1!2!2!}\times\underbrace{5\times4\times3}_{\text{choice of }S_1,S_2,S_3}=1800+10800=12600.$$

Our final answer, then, is

$$\frac{113400+75600+5400}{24}=8100.$$

■

Remark 296 *Had we sought to calculate this directly we could have counted as follows: the unused four places could have been in four different (e.g.* 123455*), three different (e.g.* 112234*) or two (e.g.* 112233*) different slots. These respectively correspond to*

$$5\times\frac{6!}{2!1!1!1!},\qquad\binom{5}{2}\binom{3}{2}\times\frac{6!}{2!2!1!1!},\qquad\binom{5}{3}\times\frac{6!}{2!2!2!}$$

arrangements to give the answer

$$1800+5400+900=8100.$$

12. REPRESENTATIONS

Theorem 297 *Given a left action of a group G on a set S there is an associated homomorphism*

$$\rho\colon G \to \mathrm{Sym}(S).$$

To each homomorphism $\rho\colon G \to \mathrm{Sym}(S)$ there is an associated left action of G on S. These correspondences are inverses of one another.

Proof. Let $g \in G$. Then the map

$$\rho_g\colon S \to S \quad \text{given by} \quad \rho_g(s) = g \cdot s$$

is a bijection of S as it has inverse $\rho_{g^{-1}}$. Further the map

$$\rho\colon G \to \mathrm{Sym}(S) \quad \text{given by} \quad g \mapsto \rho_g$$

is a homomorphism as

$$\rho_{gh}(s) = (gh) \cdot s = g \cdot (h \cdot s) = \rho_g\left(\rho_h(s)\right) = \left(\rho_g \rho_h\right)(s).$$

Conversely, given a homomorphism

$$\rho\colon G \to \mathrm{Sym}(S)$$

then there is an action of G on S given by

$$g \cdot s = \left(\rho(g)\right)(s).$$

This is a left group action as for all $s \in S$ and $g, h \in G$ we have

$$e \cdot s = \left(\rho(e)\right)(s) = id_S(s) = s$$

and

$$(gh) \cdot s = \rho(gh)(s) = \rho(g)\left(\rho(h)(s)\right) = g \cdot (h \cdot s)\,.$$

■

Corollary 298 ***(Cayley's Theorem)*** *Every finite group is isomorphic to a subgroup of some permutation group S_n. (More generally, whether or note G is finite, our proof shows that G is isomorphic to a subgroup of* $\mathrm{Sym}(G)$*.)*

Proof. As G acts on itself, by $g \cdot h = gh$, then we can consider the associated representation $\rho\colon G \to \mathrm{Sym}(G)$. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group Then $\rho(g_i)$, left multiplication by g_i, is a permutation of G. Further ρ is 1-1 as

$$\rho(g_i) = \rho(g_j) \implies \rho(g_i)(e) = \rho(g_j)(e) \implies g_i = g_j.$$

Hence G is isomorphic with the image of $\rho(G) \leqslant \mathrm{Sym}(G) \cong S_n$. ■

Example 299 *List the elements of S_3 and describe the corresponding subgroup of S_6 determined by Cayley's Theorem.*

Solution. We can list S_3 as

$$g_1 = e, \qquad g_2 = (12)\,, \qquad g_3 = (13)\,, \qquad g_4 = (23)\,, \qquad g_5 = (123)\,, \qquad g_6 = (132)\,.$$

As S_3 is generated by (12) and (13) then $\rho(S_3)$ is generated by $\rho(12)$ and $\rho(13)$. Note left-multiplication by (12) has the following effect

$$g_1 \mapsto g_2, \qquad g_2 \to g_1, \qquad g_3 \to g_5, \qquad g_4 \to g_6, \qquad g_5 \to g_3, \qquad g_6 \to g_4,$$

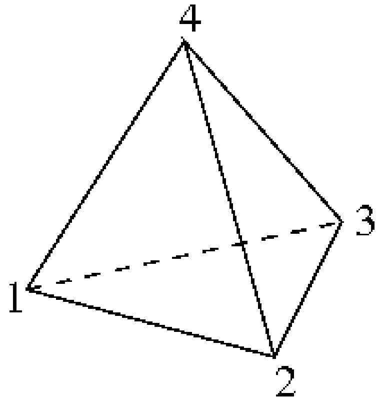
and left-multiplication by (13) has the following effect

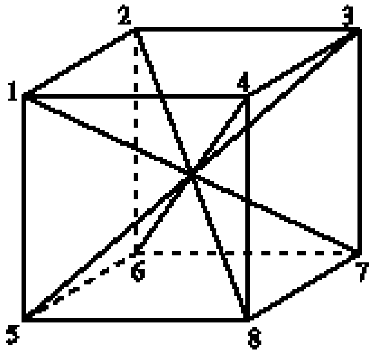
$$g_1 \mapsto g_3, \qquad g_2 \to g_6, \qquad g_3 \to g_1, \qquad g_4 \to g_5, \qquad g_5 \to g_4, \qquad g_6 \to g_2.$$

Hence $\rho(S_3)$ is the subgroup of S_6 generated by $(12)\,(35)\,(46)$ and $(13)\,(26)\,(45)$. ■

Example 300 ***Rotational Symmetry Groups of the Tetrahedron and Cube.***

Let T be a regular tetrahedron and C be a cube. We will denote as G_T the rotational symmetry group of T and as G_C the rotational symmetry group of C.





(a) If we label the four vertices of T as $1, 2, 3, 4$ then we have a homomorphism

$$\rho\colon G_T \to S_4$$

associating with each rotation in G_T the induced permutation on the labelled vertices $1, 2, 3, 4$; it is a homomorphism as composition is the binary operation in each of the two groups. Further, ρ is injective as no two distinct rotations lead to the same movement of the vertices. Hence we have an isomorphism $\rho\colon G_T \to \operatorname{Im}\rho$.

What is $\operatorname{Im}\rho$? We already know from the Orbit-Stabilizer theorem that $|G_T| = 12$ and hence it follows that

$$G_T \cong \operatorname{Im}\rho = A_4.$$

If we want to fully understand what these 12 rotations are, we see that they come in three types.

identity	:	*1 of these.*
rotation of $\pm 2\pi/3$ about a vertex and opposite face's midpoint	:	*8 of these.*
rotation of π about opposite edges' midpoints	:	*3 of these.*

The breakdown of these 12 *rotations as* $1+8+3$ *might seem at odds with the conjugacy classes of* A_4 *which we know to have sizes* $1,4,4,3$. *But note that if we are looking at a rotation of* $\pm 2\pi/3$ *about a vertex and opposite face's midpoint, and make sure to be looking down on the vertex, then we can discern clockwise rotations from anticlockwise rotations, which is why these* 8 *rotations split into two conjugacy classes and why such a rotation is not conjugate to its inverse.*

(b) If we label the vertices of C *as 1-8 then we would likewise have an injective homomorphism* $G_C \to S_8$. *However as* $|S_8| = 40320$ *it would be rather messy appreciating the structure of the image. If, instead, we consider the four diagonals of the cube*

$$D_1 = \{1,7\}, \qquad D_2 = \{2,8\}, \qquad D_3 = \{3,5\}, \qquad D_4 = \{4,6\}$$

then we have a homomorphism

$$\rho \colon G_C \to \mathrm{Sym}\{D_1, D_2, D_3, D_4\} = S_4.$$

This homomorphism is again injective. To see this we will show that its kernel is trivial. Suppose that $\rho(r) = e$ *for some rotation* $r \in G_C$. *Then* r *maps each* D_i *to* D_i *and hence maps* 1 *to either* 1 *or* 7 *and* 2 *maps to* 2 *or* 8 *etc.. If we assume that* $1 \mapsto 7$ *then* 2 *(being an adjacent vertex of* 1*) must map to* 8 *and similarly* $3 \mapsto 5$, $4 \mapsto 6$. *However the map*

$$1 \leftrightarrow 7, \qquad 2 \leftrightarrow 8, \qquad 3 \leftrightarrow 5, \qquad 4 \leftrightarrow 6$$

is not a rotation (it is $-I_3$*). So any rotation fixing the* D_i *must be the identity. As before we now have an isomorphism* $\rho \colon G_C \to \mathrm{Im}\,\rho \leqslant S_4$. *From the Orbit-Stabilizer Theorem we know that* $|G_C| = 24$ *and hence*

$$G_C \cong \mathrm{Im}\,\rho = S_4.$$

If we list the elements of G_C *we see that the rotations are:*

identity	:	*1 of these.*
rotation of $\pm\pi/2$ *about opposite faces' midpoints*	:	*6 of these.*
rotation of π *about opposite faces' midpoints*	:	*3 of these.*
rotation of $\pm\pi/3$ *about a diagonal' midpoints*	:	*8 of these.*
rotation of π *about opposite edges' midpoints*	:	*6 of these.*

and these descriptions respectively correspond to the conjugacy classes

$$\{e\}, \qquad 4\text{-cycles}, \qquad \text{double transpositions}, \qquad 3\text{-cycles}, \qquad 2\text{-cycles}.$$

Example 301 *How many ways are there to colour the faces of a cube using* n *colours?*

Solution. There are 6 faces and hence n^6 colourings. For the vertex-to-vertex rotations, the six faces split as two triples of faces (those adjacent to the vertices) which must be monochrome – hence there are n^2 such colourings fixed. For the mid-edge to mid-edge rotations, the six faces split as three pairs and so there are n^3 colourings fixed. For the mid-face to mid-face quarter turns they split as $1+1+4$, so again there are n^3 fixed colourings. Finally, for the mid-face to mid-face half turns they split as $1+1+2+2$, so there are n^4 colourings fixed.

g	fix(g)	conjugates	contribution
e	n^6	1	n^6
vertex to vertex through $\pm 2\pi/3$	n^2	8	$8n^2$
mid-edge to mid-edge	n^3	6	$6n^3$
mid-face to mid-face through $\pm\pi/2$	n^3	6	$6n^3$
mid-face to mid-face through π	n^4	3	$3n^4$

So the number of essentially different colourings of a cube's faces with n colours is

$$\frac{n^6+3n^4+12n^3+8n^2}{24}.$$

When $n=2$ compare with Example 267. ■

Example 302 *How many ways are there to colour the edges of a tetrahedron black or white, using equal numbers of each?*

Solution. The tetrahedron has six edges and so there are ${}^6C_3 = 20$ different colourings. The identity fixes all 20 of these. Given a rotation about an axis through a vertex and the opposite face's midpoint, then the six edges split as two triples than need to be of the same colour. Given a rotation about an axis through a opposite mid-points of edges, the edges split as $1+1+2+2$ so one of the 1s and one of the 2s need to be black.

g	fix(g)	conjugates	contribution
e	${}^6C_3 = 20$	1	20
vertex to face through $\pm 2\pi/3$	2	8	16
mid-edge to mid-edge	4	3	12

Thus the number of essentially different colourings is

$$\frac{20+16+12}{12} = 4.$$

■