Groups and Group Actions

Vicky Neale

Hilary Term 2020

Contents

1 Introduction

These notes are to accompany the Hilary Term 2020 Oxford Prelims course Groups and Group Actions. Specifically, they are for the first half of the course (the second half will be in Trinity Term).

This course is an introduction to group theory. We'll meet many examples of groups, and explore their properties. This will include studying permutations, and the important symmetric group. A highlight of the first half of the course will be Lagrange's theorem, which we can use to prove many interesting results, for example in number theory.

There are several resources that will help you as you study the course:

- the lectures

- these notes

- Richard Earl's notes from the 2014 course

- the problems sheets, with starter, main course and pudding problems

- the solutions to the starter and pudding problems

- each other

- tutorials in college.

In places, you will find blanks in these notes. They are there deliberately! We'll fill in these blanks during lectures. I'll also add some comments during lectures that you might want to add to these notes.

Acknowledgements

These notes, and the lectures they accompany, are extremely closely based on those produced by Dr Richard Earl. The same applies to the problems sheets. These notes are designed to match up precisely to my lectures. Richard Earl's notes are also on the course materials website, and include many additional helpful insights and examples that we don't have time to cover in lectures.

I would like these notes to be as useful as possible. If you (whether student or tutor) think that you've noticed a typo, or mistake, or part that is unclear, please check the current, up-to-date, notes on the website, to see whether I've already fixed it. If not, please email me (vicky.neale@maths) and I'll do something about it, and (with your permission) thank you here.

Thanks to Matei Iorgulescu, Mukesh Ramanathan, Paul Scarr, Edward Turner, Flora Walker, Carl Westerlund for helping to fix glitches in these notes, problems sheets and solutions.

2 Introduction to groups

Definition. Let S be a set. A *binary operation* $*$ in S is a function

$$\begin{aligned} * : S \times S &\to S \\ (a, b) &\mapsto a * b. \end{aligned}$$

Example.

- $+$, $-$, $\times$ on $\mathbb{R}$, but not $\div$ on $\mathbb{R}$
- matrix multiplication on the set $\mathcal{M}_n(\mathbb{C})$ of $n \times n$ complex matrices
- min and max on $\mathbb{N}$

- $\circ$, composition of functions, on the set $\mathrm{Sym}(X)$ of bijections from a set X to itself

Definition. We say that a binary operation $*$ on a set S is *associative* if $a * (b * c) = (a * b) * c$ for all a, b, $c \in S$.

Exercise. Which of the examples above are associative?

Definition. Let $*$ be a binary operation on a set S. We say that $e \in S$ is an *identity element* (or *identity*) if $e * a = a = a * e$ for all $a \in S$.

Exercise. Which of the examples above have an identity element?

Proposition 1. *Let $*$ be a binary operation on a non-empty set S. If there is an identity $e \in S$, then it is unique.*

Proof. Let e_1, e_2 be identity elements.
Then

$$\begin{aligned} e_1 * e_2 &= e_2 \text{ as } e_1 \text{ an identity} \\ \text{and } e_1 * e_2 &= e_1 \text{ as } e_2 \text{ an identity} \end{aligned}$$

so $e_1 = e_2$. □

Definition. Let $*$ be a binary operation on a set S, with identity e. Take $a \in S$. We say that $b \in S$ is an *inverse* for a if $a * b = e = b * a$.

Exercise. For the examples above that have an identity, which elements have inverses?

Proposition 2. *Let $*$ be an associative binary operation on a set S, with identity e. Take $a \in S$. If a has an inverse, then the inverse is unique.*

Proof. Let b, b' be inverses of a.
Then

$$\begin{aligned} b' * (a * b) &= b' * e = b' \\ \text{and } (b' * a) * b &= e * b = b, \end{aligned}$$

but $*$ is associative so these are equal, so $b = b'$. □

Definition. Let $*$ be a binary operation on a set S. Let T be a subset of S. We say that T *is closed under* $*$ if $* : T \times T \to T$ is a binary operation on T.

Remark. We can always define a restriction map $* : T \times T \to S$, but only sometimes do we have $t * t' \in T$ for all t, $t' \in T$.

Example. $+$ and $-$ are binary operations on $\mathbb{R}$, and $\mathbb{N} \subseteq \mathbb{R}$.

$\mathbb{N}$ is closed under $+$ but not under $-$.

Definition. A *group* is a set G together with a binary operation $*$ on G such that

(i) $*$ is associative;

(ii) there is an identity;

(iii) each element of G has an inverse.

Conditions (i), (ii) and (iii) are collectively called the *group axioms*.

Remark. We write the group as $(G, *)$, or simply as G when the operation is clear.

We often write the operation multiplicatively: when it will not be ambiguous, we write gh for $g * h$, and g^n for $\underbrace{ggg\cdots g}_{n \text{ times}}$ (for $n \geq 1$). With this convention, we write g^{-1} for the inverse element of g, so $g^{-1}g = e = gg^{-1}$.

(Do not use this notation if the operation is addition, when for example the inverse of g is $-g$.)

Remark. When presented with a set G and operation $*$, to show that $(G, *)$ is a group we must check the group axioms ((i), (ii), (iii) above)—but we must also ensure that $*$ is a binary operation on G, which in practice often means checking that G is closed under $*$. This is not listed as a fourth group axiom because it is part of the definition of a group that $*$ must be a binary operation on G.

Example. Which of these are groups? (We'll fill in the answers in the lecture, or you could complete the answers for yourself.)

- $(\mathbb{Z}, +)$

- $(\mathbb{N}, +)$

- $\mathcal{M}_n(\mathbb{R})$, the set of $n \times N$ real matrices, under matrix multiplication

- $GL_n(\mathbb{R})$, the set of invertible $n \times n$ real matrices, under matrix multiplication

- $(\mathbb{Q}, +)$

- $(\mathbb{Q}, \times)$

- $\{0, 1\}$ under addition modulo 2 ($0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$, $1 + 1 = 0$)

- a vector space V under $+$

Proposition 3. *Let G be a group. Let g, g_1, g_2, $g_3 \in G$, let m, $n \in \mathbb{Z}$. Then*

(i) $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$;

(ii) $(g^n)^{-1} = (g^{-1})^n$;

(iii) $g^m g^n = g^{m+n}$;

(iv) $(g^m)^n = g^{mn}$;

(v) if $g_1 g_2 = g_1 g_3$, then $g_2 = g_3$ ('cancellation on the left');

(vi) if $g_1 g_2 = g_3 g_2$, then $g_1 = g_3$ ('cancellation on the right').

Proof. Exercise, using the group axioms. □

Definition. We say that a group $(G, *)$ is *Abelian* if $g * g' = g' * g$ for all g, $g' \in G$—that is, if the binary operation $*$ is *commutative*.

Exercise. Which of the groups in the example above are Abelian?

Example.
- Let $SL_n(\mathbb{R})$ be the set of real invertible $n \times n$ matrices with determinant 1, that is, $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det A = 1\}$, the *special linear group*.

- Let $O(n)$ be the set of $n \times n$ real orthogonal matrices, that is, $O(n) = \{A \in GL_n(\mathbb{R}) : AA^T = I = A^T A\}$, the *orthogonal group*.
- Let $U(n)$ be the set of $n \times n$ unitary complex matrices, that is, $U(n) = \{A \in GL_n(\mathbb{C}) : A\overline{A}^T = I = \overline{A}^T A\}$, the *unitary group*.

Each of these is a group under matrix multiplication. Each is Abelian for $n = 1$, and non-Abelian for $n \geq 2$.

Definition. We say that a group G is *cyclic* if there is some $g \in G$ such that $G = \{g^n : n \in \mathbb{Z}\}$.

Example. $(\mathbb{Z}, +)$ is cyclic, generated by 1. It is also generated by -1.

Remark. A cyclic group must be Abelian, as $g^n g^m = g^{n+m} = g^{m+n} = g^m g^n$.

Definition. For $n \geq 1$, we define the n^{th} *cyclic group* C_n to be the set $\{e, g, g^2, \ldots, g^{n-1}\}$, where $g^n = e$, and for $0 \leq i, j \leq n-1$ we define

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

Definition. Let P_n be a regular n-gon in the plane (here $n \geq 3$). For $n \geq 3$, define the n^{th} *dihedral group* D_{2n} to be the set of isometries of the plane that send P_n to P_n. These isometries are called *symmetries* of P_n.

Exercise. Show that D_{2n} is a group under composition.

Example. $n = 3$, so P_n is an equilateral triangle.

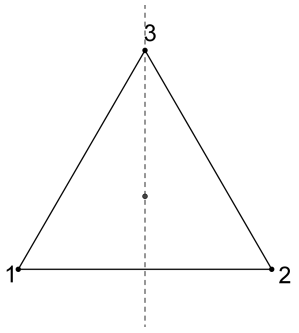

Figure 1: Equilateral triangle with vertices labelled anticlockwise from bottom left 1, 2, 3, with centre marked, and with a dashed vertical line through the top vertex 3 and the centre.

Write r for the rotation anticlockwise by $\frac{2\pi}{3}$ about the centre of the triangle, and s for the reflection in the vertical axis (see Figure 1). We can study the symmetries of P_n by considering how they permute the vertices.

$$e : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$
$$r : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$r^2 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$s : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$rs : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$r^2 s : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

These give all $3! = 6$ permutations of the vertices, so there are no further symmetries of the P_3.

So $D_6 = \{e, r, r^2, s, rs, r^2 s\}$.

Example. $n = 4$, so P_n is a square.

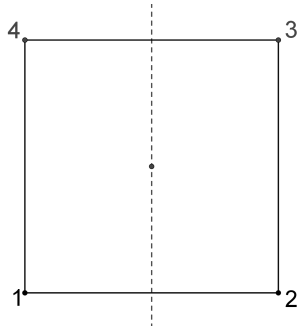

Figure 2: Square with vertices labelled anticlockwise from bottom left 1, 2, 3, 4, with centre marked, and with a dashed vertical line through the centre.

Write r for rotation anticlockwise by $\frac{\pi}{2}$ about the centre of the square, and s for reflection in the vertical axis (see Figure 2).

Exercise. Show that e, r, r^2, r^3, s, rs, $r^2 s$, $r^3 s$ are 8 distinct symmetries of the square.

We can't obtain all possible permutations of the vertices. Eg if we swap 1 and 4, then we must also swap 2 and 3, so we cannot obtain

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

So have we found all the elements of D_8?

Proposition 4. *Let P_n be a regular n-gon in the plane. Write r for rotation anticlockwise by $\frac{2\pi}{n}$ about the centre of P_n, and s for reflection in an axis of P_n. Then the symmetries of P_n are e, r, r^2, ..., r^{n-1}, s, rs, r^2s, ..., $r^{n-1}s$.*

Proof. Label the vertices of P_n anticlockwise as 1, 2, ..., n.

Let f be a symmetry of P_n, and consider $f(P_n)$.

Case 1 The vertices of $f(P_n)$ are numbered 1, 2, ..., n anticlockwise.

Say vertex 1 has moved to position k (where $1 \leq k \leq n$. Then applying $(r^{-1})^{k-1}$ will return vertex 1 to position 1, and hence all vertices to their starting positions.

So $(r^{-1})^{k-1}f = e$, so $f = r^{k-1}$.

Case 2 The vertices of $f(P_n)$ are numbered 1, 2, ..., n clockwise.

Then fs keeps the vertices in anticlockwise order, so as in Case 1 we have $fs = r^{k-1}$ for some k ($1 \leq k \leq n$), and then $f = fs^2 = r^{k-1}s$.

So the symmetries of P_n are contained in the list e, r, r^2, ..., r^{n-1}, s, rs, r^2s, ..., $r^{n-1}s$.

Now e, r, r^2, ..., r^{n-1} each send vertex 1 to a different position, and hence are all distinct.

Similarly, s, rs, r^2s, ..., $r^{n-1}s$ are all distinct.

The former collection leave the vertices in anticlockwise order, whereas the latter switch them to clockwise, so in fact all $2n$ symmetries are distinct. □

We can build new groups from old.

Definition. Given groups $(G, *_G)$ and $(H, *_H)$, we define their *product group* (or *product*) to be $(G \times H, *)$ with $*$ defined by

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

Proposition 5. *The operation $*$ just defined makes $(G \times H, *)$ into a group.*

Proof.

- closure: since $*_G$ and $*_H$ are binary operations on G and H respectively, we have $(g_1 *_G g_2, h_1 *_H h_2) \in G \times H$ for all g_1, $g_2 \in G$ and h_1, $h_2 \in H$.

- associativity: follows from the associativity of $*_G$ and $*_H$ (exercise).
- identity: the identity element in $(G \times H, *)$ is $e_{G\times H} = (e_G, e_H)$.
- inverses: given $(g, h) \in G \times H$, we have $(g, h)^{-1} = (g^{-1}, h^{-1}) \in G \times H$.

□

Definition. The *order* of a group $(G, *)$ is the cardinality $|G|$ of the set G.
If $|G|$ is finite, then we say that G is a *finite group*.

We can study finite groups using Cayley tables (and Cayley graphs).

Example. The Cayley table of D_6 is

$\downarrow \times \rightarrow$	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						
s	s	r^2s	rs	e	r^2	r
rs						
r^2s						

Some entries here have been left blank for you to complete.

This is a *Latin square*: every row and every column contains each element exactly once.

Definition. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group. The *Cayley table*, or *group table*, of G is a square $n \times n$ grid in which the entry in row i and column j is $g_i * g_j$.

Remark. G is Abelian if and only if its Cayley table is symmetrical about the $\diagdown$ (top left to bottom right) diagonal.

Proposition 6. *A Cayley table is a Latin square: each element appears exactly once in each row and in each column.*

Proof. Let G be a finite group, take $g \in G$.
Define

$$\begin{aligned} f_g : G &\to G \\ g' &\mapsto gg'. \end{aligned}$$

This is a bijection (its inverse is $g' \mapsto g^{-1}g'$).

So the entries in the row corresponding to g are precisely the elements of G in some order, each appearing exactly once.

Similarly for columns. □

Definition. Let $(G, *)$ be a group. We say that a subset $H \subseteq G$ is a *subgroup* if the restriction of $*$ to H makes H into a group, that is,

- H is closed under $*$ (if h_1, $h_2 \in H$ then $h_1 h_2 \in H$);
- H has an identity ($e_G \in H$);
- H contains inverses (if $h \in H$ then $h^{-1} \in H$).

In this case we write $H \leq G$ to mean that H is a subgroup of G.

Remark. H inherits associativity of $*$ from G, so there is no need to check this.

Definition. Let G be a group, and take $g \in G$. We define the *order* of g, $o(g)$, to be the smallest positive integer k such that $g^k = e$. If no such integer k exists, then we say that g has *infinite order*.

Remark. We have now defined the order of a group and the order of an element. These are different uses of the word 'order', although we'll see later that there are connections.

Sometimes we find that two groups have the same structure (eg the Cayley tables are essentially the same), although the elements may be labelled differently.

Definition. Let $(G, *_G)$ and $(H, *_H)$ be groups. An *isomorphism* between G and H is a bijective map $\theta : G \to H$ such that $\theta(g_1 *_G g_2) = \theta(g_1) *_H \theta(g_2)$ for all g_1, $g_2 \in G$.

If such an isomorphism exists, then we say that G and H are *isomorphic*, and write $G \cong H$.

Example. Here are some more examples of groups.

- We write $(0, \infty)$ for the set of positive real numbers, which forms a group under multiplication.
- $\mathbb{C}^* := \{z \in \mathbb{C} : z \neq 0\}$, the set of nonzero complex numbers, forms a group under multiplication.
- $S^1 := \{z \in \mathbb{C} : |z| = 1\}$, the unit circle in the complex plane, forms a group under multiplication.
- For $n \geq 1$, we define $SO(n) := \{A \in O(n) : \det A = 1\}$ to be the special orthogonal group, of orthogonal matrices with determinant 1. This forms a group under matrix multiplication.

Sheet 1 Q6 invites you to explore some potential isomorphisms involving these groups.

3 Permutations

Definition. Let S be a set. A *permutation* of S is a bijection $S \to S$. The set of permutations of S is written $\mathrm{Sym}(S)$.

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

Remark. The convention in this course is that for σ, $\tau \in S_n$ and $k \in \{1, 2, \ldots, n\}$, we write $k\sigma$ for $\sigma(k)$ and $k\sigma\tau$ for $\tau(\sigma(k))$. That is, we "write permutations on the right". You will find that some people/books write permutations on the left instead.

Theorem 7. *Let S be a set.*

(i) $\mathrm{Sym}(S)$ *is a group under composition, called the* symmetry group *of S.*

(ii) If $|S| \geq 3$, then $\mathrm{Sym}(S)$ *is non-Abelian.*

(iii) $|S_n| = n!$.

Proof. (i) Exercise.

(ii) Let x_1, x_2, x_3 be three distinct elements of S.

We seek to find two elements of $\mathrm{Sym}(S)$ that don't commute.

Define

$$\begin{aligned} f : x_1 &\mapsto x_2 \\ x_2 &\mapsto x_1 \\ x &\mapsto x \text{ for other } x \end{aligned}$$

and

$$\begin{aligned} g : x_2 &\mapsto x_3 \\ x_3 &\mapsto x_2 \\ x &\mapsto x \text{ for other } x. \end{aligned}$$

Then f, $g \in \mathrm{Sym}(S)$

and $x_1gf = x_1f = x_2$ while $x_1fg = x_2g = x_3$

so $fg \neq gf$.

(iii) To specify $f \in S_n$, we say what f does to each of 1, 2, ..., n.

There are n possibilities for $1f$,

and f is injective so there are $n - 1$ possibilities for $2f$, and so on.

This gives $n!$ possibilities for f.

□

Example. We saw previously that the elements of D_6 (the symmetries of an equilateral triangle) are the six permutations in S_3. Here we also write them using cycle notation, which we'll meet shortly.

$$\begin{aligned}
e &: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} && e \\
r &: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} && (1\ 2\ 3) \\
r^2 &: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} && (1\ 3\ 2) \\
s &: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} && (1\ 2) \\
rs &: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} && (1\ 3) \\
r^2s &: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} && (2\ 3)
\end{aligned}$$

Drawing up Cayley tables shows that D_6 and S_3 are isomorphic.

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

$$\begin{aligned}
a_i\sigma = a_{i+1} &\text{ for } 1 \leq i \leq k-1 \\
\text{and } a_k\sigma = a_1 & \\
\text{and } x\sigma = x &\text{ for } x \notin \{a_1, \ldots, a_k\}.
\end{aligned}$$

Such a cycle has *length* k. We call it a *k-cycle*. We write it as $(a_1\ a_2\ \ldots\ a_k)$.

Remark.

- A k-cycle has order k.
- We often call a 2-cycle a *transposition*.

Example. In S_5, (1 2 3) and (2 4 5 1 3) = (5 1 3 2 4) are cycles (3-cycle and 5-cycle respectively), but (1 2 3)(4 5) is not a cycle.

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

Proposition 8. *Let $\alpha = (a_1 \ldots a_k)$ and $\beta = (b_1 \ldots b_l)$ be disjoint cycles. Then α and β commute.*

Proof. We have

$$\begin{aligned} a_i\alpha\beta = a_{i+1}\beta = a_{i+1} \text{ for } 1 \le i \le k-1 \\ \text{and } a_i\beta\alpha = a_i\alpha = a_{i+1} \text{ for } 1 \le i \le k-1 \\ \text{and } a_k\alpha\beta = a_1\beta = a_1 \\ \text{and } a_k\beta\alpha = a_k\alpha = a_1 \\ \text{and similarly } b_j\alpha\beta = b_j\beta\alpha \text{ for } 1 \le j \le l, \end{aligned}$$

and for $x \notin \{a_1, \ldots, a_k, b_1, \ldots, b_l\}$ we have $x\alpha\beta = x = x\beta\alpha$.

So $\alpha\beta = \beta\alpha$. □

Example. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 9 & 7 & 3 & 2 & 4 & 8 & 1 \end{pmatrix} \in S_9.$$

Have

$$\begin{aligned} 1 \to 5 \to 3 \to 9 \to 1 \\ \text{and } 2 \to 6 \to 2 \\ \text{and } 4 \to 7 \to 4 \\ \text{and } 8 \to 8 \end{aligned}$$

so $\sigma = (1\ 5\ 3\ 9)(2\ 6)(4\ 7)(8)$ as a product of disjoint cycles.

Then $\sigma^{-1} = (1\ 9\ 3\ 5)(2\ 6)(4\ 7)(8)$

and $\sigma^{101} = (1\ 5\ 3\ 9)^{101}(2\ 6)^{101}(4\ 7)^{101}(8)^{101} = (1\ 5\ 3\ 9)(2\ 6)(4\ 7)(8)$.

Theorem 9. *Every permutation in S_n can be written as a product of disjoint cycles. Moreover, this product is unique up to cycling elements without cycles and permuting the order of the cycles.*

Proof. Take $\sigma \in S_n$.

Existence: Take $a_1 \in \{1, 2, \ldots, n\}$. Consider a_1, $a_1\sigma$, $a_1\sigma^2$, ...

All of these are in the finite set $\{1, 2, \ldots, n\}$, so we must have $a_1\sigma^r = a_1\sigma^s$ for some r, s with $r < s$.

Then $a_1 = a_1\sigma^{s-r}$, so in fact a_1 is the first element to be repeated.

Say k_1 is the smallest positive integer with $a_1\sigma^{k_1} = a_1$.

Then σ permutes $\{a_1, a_1\sigma, a_1\sigma^2, \ldots, a_1\sigma^{k_1-1}\}$ (the *orbit* of a_1) via the cycle $(a_1\ a_1\sigma\ a_1\sigma^2\ \ldots\ a_1\sigma^{k_1-1})$.

If $k_1 = n$, then $\sigma = (a_1\ a_1\sigma\ a_1\sigma^2\ \ldots\ a_1\sigma^{k_1-1})$ is a cycle and we are done.

If not, then there is a_2 not in the orbit of a_1. Repeating the same argument shows that σ permutes the orbit of a_2 via a cycle.

The two cycles must be disjoint, because if $a_1\sigma^i = a_2\sigma^j$ then $a_2 = a_1\sigma^{i-j}$ is in the orbit of a_1, which it isn't.

Continuing in this way, we obtain σ as a product of disjoint cycles. The process must stop, because $\{1, 2, \ldots, n\}$ is finite so eventually the orbits will use it all up.

Uniqueness: Suppose that $\sigma = \pi_1 \cdots \pi_r = \tau_1 \cdots \tau_s$

where $\pi_1, \ldots, \pi_r$ are disjoint cycles

and $\tau_1, \ldots, \tau_s$ are disjoint cycles.

Then 1 appears in exactly one π_i, without loss of generality say it's π_1 (if necessary reorder the cycles, which is allowed since they commute),

and similarly 1 appears in exactly one τ_j, say τ_1.

Now without loss of generality 1 appears at the start of π_1 and τ_1 (if necessary cycle elements within the cycle).

Then $1\sigma = 1\pi_1 = 1\tau_1$ and so on,

and so $\pi_1 = \tau_1 = (1\ 1\sigma\ 1\sigma^2\ \ldots\ 1\sigma^{k-1})$ where k is the size of the orbit of 1 under σ.

Repeating with an element not in the orbit of 1 shows that $\pi_2 = \tau_2$ and so on.

So in fact the decomposition into disjoint cycles are the same. □

Remark. We often do not record 1-cycles, eg $\sigma = (1\ 5\ 3\ 9)(2\ 6)(4\ 7)(8)$ is usually written as $(1\ 5\ 3\ 9)(2\ 6)(4\ 7)$.

Definition. For a given permutation $\sigma \in S_n$, Theorem 9 shows that the lengths of the cycles of σ (when written as a product of disjoint cycles) are well defined. This is called the *cycle type* of σ.

Example. The permutation $(1\ 5\ 3\ 9)(2\ 6)(4\ 7) \in S_9$ has cycle type 4, 2, 2, 1.

Proposition 10. *Let $\pi \in S_n$ be written as $\pi = \sigma_1\sigma_2 \cdots \sigma_k$ as a product of disjoint cycles. For $1 \leq i \leq k$, let l_i be the length of σ_i. Then the order of π is* $\mathrm{lcm}(l_1, \ldots, l_k)$. *"cycle type determines order"*

Proof. Exercise. □

Definition. We say that two permutations $\sigma, \tau \in S_n$ are *conjugate* if there is some $\rho \in S_n$ with $\sigma = \rho^{-1}\tau\rho$.

Lemma 11. *Let $(a_1\ a_2\ \ldots\ a_k)$ be a cycle in S_n, and take $\sigma \in S_n$. Then*

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

Proof. Exercise (on Sheet 2). □

Theorem 12. *Let σ, $\tau \in S_n$. They are conjugate if and only if they have the same cycle type.*

Proof. ($\Rightarrow$) Assume that σ, τ are conjugate, so there is $\rho \in S_n$ such that $\sigma = \rho^{-1}\tau\rho$.

Say $\tau = \pi_1 \cdots \pi_r$ where the π_i are disjoint cycles.

By Lemma 11, $\rho^{-1}\pi_i\rho$ is a cycle of the same length as π_i.

But $\sigma = \rho^{-1}\tau\rho = \rho^{-1}\pi_1\rho\rho^{-1}\pi_2\rho\cdots\rho^{-1}\pi_r\rho$

so σ has the same cycle type as τ.

($\Leftarrow$) Assume that σ and τ have the same cycle type, say

$$\sigma = (a_1 \ \ldots \ a_{k_1})(a_{k_1+1} \ \ldots \ a_{k_2})\cdots(a_{k_{m-1}+1} \ \ldots \ a_{k_m})$$
$$\text{and } \tau = (b_1 \ \ldots \ b_{k_1})(b_{k_1+1} \ \ldots \ b_{k_2})\cdots(b_{k_{m-1}+1} \ \ldots \ b_{k_m}).$$

Define $\rho \in S_n$ as follows: define $a_i\rho = b_i$ for $1 \leq i \leq k_m$.

Then, by Lemma 11, $\rho^{-1}(a_1 \ \ldots \ a_{k_1})\rho = (b_1 \ \ldots \ b_{k_1})$ and so on,

so $\rho^{-1}\sigma\rho = \tau$, so σ and τ are conjugate. □

Definition. An $n \times n$ matrix is a *permutation matrix* if each row and each column contains exactly one entry that is 1, with all other entries 0.

Remark. Take $\sigma \in S_n$. We obtain a corresponding permutation matrix P_σ by specifying that the nonzero entry in row i is a 1 in column $i\sigma$. So P_σ has i, j entry $\delta_{i\sigma,j}$. Note that P_σ genuinely *is* a permutation matrix.

Example. In S_3, we have

$$P_{(1\ 2)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$P_{(1\ 3\ 2)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Lemma 13. *If σ, $\tau \in S_n$, then $P_{\sigma\tau} = P_\sigma P_\tau$.*

Proof. The i,j entry of $P_\sigma P_\tau$ is

$$\begin{aligned}(P_\sigma P_\tau)_{i,j} &= \sum_{k=1}^{n} (P_\sigma)_{i,k}(P_\tau)_{k,j} \text{ (definition of matrix multiplication)} \\ &= \sum_{k=1}^{n} \delta_{i\sigma,k}\delta_{k\tau,j} \\ &= \delta_{i\sigma\tau,j} \\ &= (P_{\sigma\tau})_{i,j}.\end{aligned}$$

□

Lemma 14. *If $\sigma \in S_n$ is a transposition, then* $\det(P_\sigma) = -1$.

Proof. Say $\sigma = (i\ j)$.
Then P_σ is I_n with rows i and j swapped,
so $\det(P_\sigma) = -\det(I_n) = -1$. □

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

Theorem 15. *(i) Any permutation in S_n can be written as a product of transpositions.*

(ii) A permutation cannot be both even and odd.

Proof. (i) Any permutation in S_n can be written as a product of disjoint cycles (Theorem 9), so we concentrate on an arbitrary cycle $(a_1\ a_2\ \ldots\ a_k)$.

We have

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_2)(a_1\ a_3)\cdots(a_1\ a_k).$$

(ii) Say $\sigma = \tau_1 \cdots \tau_k$ where $\tau_1, \ldots, \tau_k$ are transpositions.

Then

$$\begin{aligned}\det(P_\sigma) &= \det(P_{\tau_1} \cdots P_{\tau_k}) \text{ by Lemma 13} \\ &= \det(P_{\tau_1}) \cdots \det(P_{\tau_k}) \text{ as det multiplicative} \\ &= (-1)^k \text{ by Lemma 14.}\end{aligned}$$

So σ cannot be both even and odd.

□

Remark. From this, we see that a cycle is odd if and only if it has even length.

So a permutation is even if and only if its cycle type has an even number of cycles of even length.

Also, (ii) shows that σ is even if and only if $\det(P_\sigma) = 1$.

Definition. For $n \geq 1$, define $A_n := \{\sigma \in S_n : \sigma \text{ is even }\}$, the n^{th} *alternating group.*

Proposition 16. *(i) A_n is a subgroup of S_n.*

(ii) For $n \geq 2$, the order of A_n is $\frac{1}{2}n!$.

(iii) For $n \geq 4$, A_n is non-Abelian.

Proof. (i) – Closure: Take $\sigma, \tau \in A_n$, so σ and τ are even.
Then $\det(P_\sigma) = \det(P_\tau) = 1$ by Theorem 15,
so $\det(P_{\sigma\tau}) = \det(P_\sigma P_\tau) = \det(P_\sigma)\det(P_\tau) = 1$ (using Lemma 13),
so $\sigma\tau$ is even so $\sigma\tau \in A_n$.

– Identity: Note that e (the identity permutation) is a product of 0 transpositions and hence even, so $e \in A_n$.

– Inverses: Take $\sigma \in A_n$. Then

$$\begin{aligned}\det(P_\sigma P_{\sigma^{-1}}) &= \det(P_\sigma)\det(P_{\sigma^{-1}}) \\ &= \det(P_{\sigma^{-1}}),\end{aligned}$$

but also

$$\begin{aligned}\det(P_\sigma P_{\sigma^{-1}}) &= \det(I_n) \\ &= 1,\end{aligned}$$

so σ^{-1} is even so $\sigma^{-1} \in A_n$.

So $A_n \leq S_n$.

(ii) Define

$$\begin{aligned}f : A_n &\to S_n \setminus A_n \\ \sigma &\mapsto (1\ 2)\sigma.\end{aligned}$$

Note that f is well defined: if σ is even, then $(1\ 2)\sigma$ is odd.
And f is a bijection: it has inverse $\sigma \mapsto (1\ 2)\sigma$.
So $|A_n| = |S_n \setminus A_n| = |S_n| - |A_n|$, so $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$.

(iii) For $n \geq 4$, $(1\ 2\ 3)$ and $(1\ 2\ 4)$ are elements of A_n.
Now

$$(1\ 2\ 3)(1\ 2\ 4) =$$
$$\text{while } (1\ 2\ 4)(1\ 2\ 3) =$$

so A_n is non-Abelian.
These products have been left blank for you to fill in.

□

Remark. In S_n, two permutations are conjugate if and only if they have the same cycle type. This is not true in A_n. If two elements are conjugate in A_n, then they are conjugate in S_n and so have the same cycle type. But it is possible for two elements of A_n to have the same cycle type without being conjugate in A_n. For example, (1 2 3) and (1 3 2) are not conjugate in A_4 (exercise: show this).

4 Subgroups

Proposition 17 (Subgroup test)**.** *Let G be a group. The subset $H \subseteq G$ is a subgroup of G if and only if H is non-empty and $h_1 h_2^{-1} \in H$ for all h_1, $h_2 \in H$.*

Proof. ($\Rightarrow$) Assume that H is a subgroup of G.
Then $e \in H$, so H is non-empty.
Also, if h_1, $h_2 \in H$ then $h_2^{-1} \in H$ as H contains inverses
so $h_1 h_2^{-1} \in H$ as H is closed under the group operation.
($\Leftarrow$) Assume that H is non-empty, say $h \in H$, and that $h_1 h_2^{-1} \in H$ for all h_1, $h_2 \in H$.

- Identity: Have $hh^{-1} = e \in H$.
- Inverses: Take $h_1 \in H$. Have $eh^{-1} = h_1^{-1} \in H$.
- Closure: Take h_1, $h_2 \in H$. Then $h_2^{-1} \in H$ so $h_1 (h_2^{-1})^{-1} = h_1 h_2 \in H$.

So $H \leq G$. □

Proposition 18. *Let G be a group. Let H, K be subgroups of G. Then $H \cap K$ is a subgroup of G.*

Proof. Exercise. □

Remark. We can extend this to show that for any index set I, if H_i (for $i \in I$) are subgroups of a group G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Definition. Let G be a group. Let S be a subset of G. The *subgroup generated by S*, written $\langle S \rangle$, is the smallest subgroup of G that contains S, that is,

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H.$$

The elements of S are called the *generators* of $\langle S \rangle$.

Remark. For $g \in G$, we write $\langle g \rangle$ for $\langle \{g\} \rangle$.

Example. $G = \mathbb{Z}$, $S = \{14, 21\}$.
We have $7 = 21 - 14 \in \langle S \rangle$, so $\langle S \rangle$ contains all multiples of 7.
Also, every element of $\langle S \rangle$ is a multiple of 7.
So $\langle S \rangle = 7\mathbb{Z}$.

Division algorithm Let a, b be integers with $b > 0$. Then there are unique integers q and r such that $a = qb + r$ and $0 \leq r < b$.

Proposition 19. *Let G be a group. Take $g \in G$.*

(i) We have $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$.

(ii) If g has finite order, then $\langle g \rangle = \{e, g, g^2, \ldots, g^{o(g)-1}\}$.

Proof. (i) $\supseteq$: Clearly if $k \in \mathbb{Z}$ then $g^k \in \langle g \rangle$, so $\langle g \rangle \supseteq \{g^k : k \in \mathbb{Z}\}$.

$\subseteq$:

Claim. $H = \{g^k : k \in \mathbb{Z}\}$ is a subgroup of G.

Proof of claim

- We have $e = g^0 \in H$ so H is non-empty.
- If g^k, $g^l \in H$, then $(g^k)(g^l)^{-1} = g^{k-l} \in H$.

So by subgroup test have $H \leq G$, which proves the claim.

So $\langle g \rangle \subseteq H$.

So $\langle g \rangle = H$.

(ii) Let $d = o(g)$.

$\supseteq$: Clearly $\langle g \rangle \supseteq \{e, g, \ldots, g^{d-1}\}$.

$\subseteq$: Take $g^k \in \langle g \rangle$.

By the division algorithm, we have $k = qd + r$ for some q, $r \in \mathbb{Z}$ with $0 \leq r \leq d - 1$.

Then $g^k = g^{qd+r} = (g^d)^q g^r = g^r \in \{e, g, \ldots, g^{d-1}\}$.

So $\langle g \rangle \subseteq \{e, g, \ldots, g^{d-1}\}$.

So $\langle g \rangle = \{e, g, \ldots, g^{d-1}\}$.

□

Remark. So a group G is cyclic precisely when there is some $g \in G$ such that $G = \langle g \rangle$.

In particular, a finite group G is cyclic if and only if there is some $g \in G$ with $o(g) = |G|$.

Example.

- $C_5 = \{e, g, g^2, g^3, g^4\}$ is generated by any one of g, g^2, g^3, g^4.
- $C_6 = \{e, g, g^2, g^3, g^4, g^5\}$ is generated by either of g, g^5.
- $C_2 \times C_2$ is not cyclic: it has order 4, but contains no element of order 4.

Theorem 20. *Let G be a cyclic group, say $G = \langle g \rangle$.*

(i) If G is finite, with $|G| = n$, then $G \cong C_n$.

(ii) If G is infinite, then $G \cong \mathbb{Z}$.

Proof. (i) We see that g has order n, and $G = \{e, g, \ldots, g^{n-1}\} \cong C_n$.

(ii) Define

$$\begin{aligned} \theta : G &\to \mathbb{Z} \\ g^k &\mapsto k. \end{aligned}$$

This is an isomorphism.

□

Theorem 21. *Let G be a cyclic group. Let H be a subgroup of G. Then H is cyclic.*

Proof. Say $G = \langle g \rangle$.

If $H = \{e\}$, then H is cyclic and we are done.

So suppose not, so $g^k \in H$ for some $k \in \mathbb{Z} \setminus \{0\}$.

Then we must have $g^l \in H$ for some $l \in \mathbb{Z}^{>0}$, because if $g^k \in H$ then also $g^{-k} \in H$.

Let $d = \min\{m \in \mathbb{Z}^{>0} : g^m \in H\}$.

Then certainly $\langle g^d \rangle \subseteq H$.

Take $g^n \in H$. By the division algorithm, there are $q, r \in \mathbb{Z}$ with $n = qd + r$ and $0 \leq r < d$.

Then $g^n = g^{qd+r}$, so $g^r = g^{n-qd} = g^n (g^d)^{-q} \in H$.

Since $0 \leq r < d$ and d is minimal, we must have $r = 0$. That is, d divides n, and so $g^n \in \langle g^d \rangle$.

So $H = \langle g^d \rangle$ is cyclic. □

Remark. Applying this to the cyclic group $\mathbb{Z}$ shows that every subgroup of $\mathbb{Z}$ is of the form $\langle m \rangle = m\mathbb{Z}$ for some integer m.

Consequently, given any two integers m and n, there are integers h and l such that

$$\langle m, n \rangle = \langle h \rangle \text{ and } \langle m \rangle \cap \langle n \rangle = \langle l \rangle.$$

We may assume that h and l are positive.

Example. $m = 14$, $n = 21$. Then $\langle 14, 21 \rangle = \langle 7 \rangle$ and $\langle 14 \rangle \cap \langle 21 \rangle = \langle 42 \rangle$, so we can take $h = 7$, $l = 42$.

Proposition 22. *Let m, n be integers. Let h, l be positive integers such that $\langle m, n \rangle = \langle h \rangle$ and $\langle m \rangle \cap \langle n \rangle = \langle l \rangle$. Then*

(i) $h \mid m$ and $h \mid n$ (that is, h is a common factor *of m and n);*

*(ii) there are a, $b \in \mathbb{Z}$ such that $h = am + bn$ (*Bézout's lemma*);*

(iii) if $d \mid m$ and $d \mid n$, then $d \mid h$ (that is, h is divisible by every common factor of m and n);

(iv) $m \mid l$ and $n \mid l$ (that is, l is a common multiple *of m and n);*

(v) if $m \mid c$ and $n \mid c$, then $l \mid c$ (that is, any common multiple of m and n is a multiple of l).

Proof. (i) We have $m \in \langle m, n \rangle = \langle h \rangle$, so $m = kh$ for some $k \in \mathbb{Z}$ so $h \mid m$. Similarly $h \mid n$.

(ii) We have $h \in \langle h \rangle = \langle m, n \rangle$ so $h = am + bn$ for some a, $b \in \mathbb{Z}$ (here we use that $\mathbb{Z}$ is Abelian).

(iii) Suppose that $d \mid m$ and $d \mid n$. Then $d \mid (rm + sn)$ for any r, $s \in \mathbb{Z}$. So from (ii) we have $d \mid h$.

(iv) We have $l \in \langle l \rangle$, so $l \in \langle m \rangle$ and $l \in \langle n \rangle$ so $m \mid l$ and $n \mid l$.

(v) Suppose that $m \mid c$ and $n \mid c$. Then $c \in \langle m \rangle$ and $c \in \langle n \rangle$, so $c \in \langle m \rangle \cap \langle n \rangle = \langle l \rangle$. So $l \mid c$.

□

Definition. We define h here to be the *highest common factor* (*hcf*) of m and n, and l to be the *least common multiple* (*lcm*) of m and n.

Lemma 23. *Let G be a group, let $g \in G$ be an element with finite order d. We have $g^k = e$ if and only if $d \mid k$.*

Proof. ($\Leftarrow$) Assume that $d \mid k$, say $k = ad$ where $a \in \mathbb{Z}$.

Then $g^k = (g^d)^a = e$.

($\Rightarrow$) Assume that $g^k = e$.

By the division algorithm, we have $k = qd + r$ for some integers q, r with $0 \leq q < d$.

Then $g^r = g^{k-qd} = g^k(g^d)^q = e$.

Since $r < d$ and d is minimal, we have $r = 0$.

So $d \mid k$. □

Theorem 24 (Chinese Remainder Theorem)**.** *Let m, n be coprime positive integers (that is, they have hcf 1). Then $C_m \times C_n$ is cyclic, and is isomorphic to C_{mn}.*

Proof. Say $C_m = \langle g \rangle$ and $C_n = \langle h \rangle$.

Claim. $(g, h) \in C_m \times C_n$ has order mn.

Proof of claim We have $(g, h)^{mn} = ((g^m)^n, (h^n)^m)) = (e, e)$, so the order of (g, h) is at most mn.

Also, for any $k \in \mathbb{Z}^{>0}$ if $(g, h)^k = (e, e)$ then $g^k = e$ and $h^k = e$.

So $m \mid k$ and $n \mid k$, by Lemma 23.

Since m and n are coprime, by Bézout there are integers a and b such that $am + bn = 1$.

Then $akm + bkn = k$, and both terms on the left are divisible by mn, so $mn \mid k$, so $k \geq mn$.

So the order of (g, h) is mn, which proves the claim.

Now $|C_m \times C_n| = mn$, so $C_m \times C_n$ is a group of order mn containing an element with order mn, so $C_m \times C_n$ is cyclic and $C_m \times C_n \cong C_{mn}$. □

5 Equivalence relations

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

For a relation $R \subseteq S \times S$, we write aRb if and only if $(a, b) \in R$.

Definition. Let $\sim$ be a relation on a set S. We say that $\sim$ is an *equivalence relation* if

- $\sim$ is *reflexive* (that is, if $a \sim a$ for all $a \in S$);
- $\sim$ is *symmetric* (that is, if $a \sim b$ then $b \sim a$);
- $\sim$ is *transitive* (that is, if $a \sim b$ and $b \sim c$, then $a \sim c$).

Example.
- $S = GL_n(\mathbb{R})$, with $A \sim B$ if and only if there is $P \in GL_n(\mathbb{R})$ with $A = P^{-1}BP$.
- S is a group, with $x \sim y$ if and only if $x = y$ or $x = y^{-1}$.

Proposition 25. *Let $n \geq 2$ be an integer. Define a relation $\sim$ on $\mathbb{Z}$ by $a \sim b$ if and only if $a - b$ is a multiple of n. Then $\sim$ is an equivalence relation.*

Proof. Take a, b, $c \in \mathbb{Z}$.

- reflexive: $a - a$ is a multiple of n.
- symmetric: if n divides $a - b$ then n divides $b - a$.
- transitive: if n divides $a - b$ and $b - c$, say $a - b = kn$ and $b - c = ln$ where k, $l \in \mathbb{Z}$, then $a - c = (a - b) + (b - c) = (k + l)n$ so n divides $a - c$.

□

Definition. The equivalence relation in Proposition 25 is called *congruence modulo n*.

Definition. Let G be a group. We say that g_1, $g_2 \in G$ are *conjugate* if there is $h \in G$ with $g_1 = h^{-1}g_2h$.

Proposition 26. *Let G be a group. Conjugacy in G is an equivalence relation.*

Proof. Write $h \sim k$ if and only if h and k are conjugate in G (that is, if and only if there is $g \in G$ with $h = g^{-1}kg$).

Take g_1, g_2, $g_3 \in G$.

- reflexive: have $g_1 = e^{-1}g_1e$ so $g_1 \sim g_1$.
- symmetric: if $g_1 \sim g_2$, then there is $h \in G$ with $g_1 = h^{-1}g_2h$. Then $g_2 = hg_1h^{-1} = (h^{-1})^{-1}g_1(h^{-1})$ so $g_2 \sim g_1$.
- transitive: if $g_1 \sim g_2$ and $g_2 \sim g_3$, then there are h_1, $h_2 \in G$ with $g_1 = h_1^{-1}g_2h_1$ and $g_2 = h_2^{-1}g_3h_2$.

  Then $g_1 = h_1^{-1}(h_2^{-1}g_3h_2)h_1 = (h_2h_1)^{-1}g_3(h_2h_1)$, so $g_1 \sim g_3$.

□

Definition. Let $\sim$ be an equivalence relation on a set S. For $a \in S$, we define the *equivalence class* of a, written $[a]$ or $\overline{a}$, to be the set $\{b \in S : a \sim b\}$. "all the things related to a."

Example. The equivalence classes for congruence modulo n are

$$\begin{aligned}\overline{0} &= n\mathbb{Z}\\ \overline{1} &= 1 + n\mathbb{Z}\\ \overline{2} &= 2 + n\mathbb{Z}\\ &\vdots\\ \overline{n-1} &= (n-1) + n\mathbb{Z}\end{aligned}$$

—by the division algorithm, this is all.

Example. For a permutation $\sigma \in S_n$, its equivalence class under conjugation in S_n is its *conjugacy class*, which, as we saw, consists precisely of those permutations in S_n that have the same cycle type as σ.

Definition. Let S be a set, let I be an index set. For $i \in I$, let S_i be a subset of S. We say that the S_i (for $i \in I$) *partition* S if

- $S_i \neq \emptyset$ for all $i \in I$ (non-empty);
- $\bigcup_{i \in I} S_i = S$ (cover);
- $S_i \cap S_j = \emptyset$ for $i \neq j$ (pairwise disjoint).

Theorem 27. *Let $\sim$ be an equivalence relation on a set S. The equivalence classes of $\sim$ partition S.*

Proof.
- Non-empty: for any $a \in S$, we have $a \in [a]$ as $\sim$ is reflexive, so each equivalence class is non-empty.
- Cover: since $a \in [a]$ for all $a \in S$, certainly $\bigcup_{a \in S} [a] = S$.
- Pairwise disjoint: take $a, b \in S$. Aim: $[a] = [b]$ or $[a] \cap [b] = \emptyset$
  Suppose $c \in [a] \cap [b]$. Aim: $[a] = [b]$
  Then $a \sim c$ and $b \sim c$, so by symmetry $c \sim b$, so by transitivity $a \sim b$.
  If $d \in [b]$, then $b \sim d$, so by transitivity $a \sim d$, so $d \in [a]$. So $[b] \subseteq [a]$.
  Similarly, $[a] \subseteq [b]$.
  So either $[a] \cap [b] = \emptyset$ or $[a] = [b]$.

□

Given an equivalence relation on a set S, we obtain a partition of S. We can go the other way too.

Theorem 28. *Let P be a partition of a set S. For $a \in S$, write P_a for the unique part in P with $a \in P_a$. Define a relation $\sim$ on S by $a \sim b$ if and only if $b \in P_a$. Then $\sim$ is an equivalence relation.*

Proof. Take a, b, $c \in S$.

- reflexive: we have $a \in P_a$ so $a \sim a$.
- symmetric: if $a \sim b$ then $b \in P_a$, so $b \in P_a \cap P_b$, so $P_a \cap P_b \neq \emptyset$, so $P_a = P_b$, so $a \in P_b$, so $b \sim a$.
- transitive: if $a \sim b$ and $b \sim c$, then $b \in P_a \cap P_b$ and so $P_a = P_b$, but also $c \in P_b$, so $c \in P_a$ so $a \sim c$.

□

Corollary 29. *There is a bijection between equivalence relations on a set S and partitions of that same set S.*

Proof. Theorem 27 gives a map in one direction, and a quick check shows that Theorem 28 gives the inverse. □

We saw in Proposition 25 that congruence modulo n is an equivalence relation on $\mathbb{Z}$. We write $a \equiv b \pmod{n}$ to mean that a and b are congruent modulo n. We noted that the equivalence classes are $\overline{0}$, $\overline{1}$, …, $\overline{n-1}$. Write $\mathbb{Z}_n$ for the set of these equivalence classes. (Note that $\mathbb{Z}_n$ is not a subset of $\mathbb{Z}$.)

Definition. Define binary operations $+$ and $\times$ on $\mathbb{Z}_n$ by

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\text{and } \overline{a} \times \overline{b} = \overline{a \times b}.$$

Lemma 30. *The operations $+$ and $\times$ on $\mathbb{Z}_n$ are well defined.*

Remark. The concern here is what happens if we have potentially different representatives of the same equivalence class, say $\overline{a} = \overline{c}$ and $\overline{b} = \overline{d}$. We want to know that $\overline{a+b} = \overline{c+d}$ and $\overline{a \times b} = \overline{c \times d}$.

Proof. Assume that $\overline{a} = \overline{c}$ and $\overline{b} = \overline{d}$.

Then $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$,

so there are k, $l \in \mathbb{Z}$ such that $a - c = kn$ and $b - d = ln$.

Then $(a+b) - (c+d) = (a-c) + (b-d) = (k+l)n$ so $a + b \equiv c + d \pmod{n}$,

and $(a \times b) - (c \times d) = ab - (a - kn)(b - ln) = (bk + al - kln)n$ so $ab \equiv cd \pmod{n}$,

so $\overline{a+b} = \overline{c+d}$ and $\overline{a \times b} = \overline{c \times d}$. □

Proposition 31. *$(\mathbb{Z}_n, +)$ is an Abelian group. Moreover, it is cyclic and isomorphic to C_n.*

Furthermore, $\times$ is associative and commutative on $\mathbb{Z}_n$, and $\times$ is distributive over $+$.

Proof. Exercise. Check that the relevant properties transfer across from $\mathbb{Z}$.

Note that $\overline{1}$ has order n in $\mathbb{Z}_n$, so $(\mathbb{Z}_n, +)$ is cyclic generated by $\overline{1}$. □

Proposition 32. *(i) Take $\overline{x} \in \mathbb{Z}_n$. Then $\overline{x}$ has a multiplicative inverse in $\mathbb{Z}_n$ (that is, there exists $\overline{y} \in \mathbb{Z}_n$ with $\overline{x}\ \overline{y} = \overline{1}$) if and only if* $\mathrm{hcf}(x, n) = 1$.

(ii) If p is prime, then $\mathbb{Z}_p$ is a field.

(iii) Let $\mathbb{Z}_n^\times = \{\overline{x} \in \mathbb{Z}_n : \overline{x}$ has a multiplicative inverse$\}$ be the set of units *in $\mathbb{Z}_n$. Then $\mathbb{Z}_n^\times$ is a group under multiplication.*

Proof. Exercise (see Sheet 4). □

6 Cosets and Lagrange's Theorem

Definition. Let G be a group, let H be a subgroup of G. A *left coset* of H in G is a set $gH := \{gh : h \in H\}$ where $g \in G$. The set of left cosets of H in G is denoted G/H. The cardinality of this set is called the *index* of H in G. A *right coset* of H in G is a set $Hg := \{hg : h \in H\}$ where $g \in G$.

Remark. If G is Abelian, then left cosets and right cosets are the same thing. If G is not Abelian, then we may or may not have $gH = Hg$ for any given $g \in G$.

Example. $G = \mathbb{Z}$, $H = n\mathbb{Z}$.

The left coset of r is $r + n\mathbb{Z}$ (note that we write this coset additively, because the group operation is addition).

The cosets (left and right as G is Abelian) are $n\mathbb{Z}$, $1+n\mathbb{Z}$, $\ldots$, $(n-1)+n\mathbb{Z}$.

This looks a lot like $\mathbb{Z}_n \ldots$.

Example. $G = S_3$, $H = \langle(1\ 2)\rangle = \{e, (1\ 2)\}$. The left cosets are

$$\begin{aligned}
eH &= H \\
(1\ 2)H &= H \\
(1\ 3)H &= \{(1\ 3), (1\ 3)(1\ 2)\} = \{(1\ 3), (1\ 3\ 2)\} \\
(2\ 3)H &= \{(2\ 3), (2\ 3)(1\ 2)\} = \{(2\ 3), (1\ 2\ 3)\} \\
(1\ 2\ 3)H &= \{(1\ 2\ 3), (1\ 2\ 3)(1\ 2)\} = \{(1\ 2\ 3), (2\ 3)\} \\
(1\ 3\ 2)H &= \{(1\ 3\ 2), (1\ 3\ 2)(1\ 2)\} = \{(1\ 3\ 2), (1\ 3)\},
\end{aligned}$$

so H has index 3 in G.

Lemma 33 (Coset equality test)**.** *Let H be a subgroup of a group G. Take g_1, $g_2 \in G$. We have $g_1H = g_2H$ if and only if $g_2^{-1}g_1 \in H$.*

Proof. ($\Rightarrow$) Assume that $g_1H = g_2H$.
Then $g_1 = g_1e \in g_1H$ so $g_1 \in g_2H$ so there is $h \in H$ with $g_1 = g_2h$.
Then $g_2^{-1}g_1 = h \in H$.
($\Leftarrow$) Assume that $g_2^{-1}g_1 \in H$, say $g_2^{-1}g_1 = h \in H$. Aim: show sets g_1H and g_2H are equal
Take an element of g_1H, say g_1h_1 where $h_1 \in H$. Aim: show $g_1h_1 \in g_2H$
Then $g_2^{-1}g_1h_1 = hh_1 \in H$ so $g_1h_1 = g_2hh_1 \in g_2H$
So $g_1H \subseteq g_2H$.
Since $g_1^{-1}g_2 = h^{-1} \in H$, we similarly obtain $g_2H \subseteq g_1H$.
So $g_1H = g_2H$. □

Theorem 34 (Lagrange's Theorem)**.** *Let G be a finite group and let H be a subgroup of G. Then $|H| \mid |G|$.*
"the order of a subgroup divides the order of the group"

Proof.

Claim. The left cosets of H partition G.
Proof of claim

- Non-empty: we have $g \in gH$ so $gH \neq \emptyset$ for all $g \in G$.
- Cover: since $g \in gH$ for all $g \in G$, we have $\bigcup_{g \in G} gH = G$.
- Pairwise disjoint: take g_1, $g_2 \in G$. Aim: $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$
  Suppose $g \in g_1H \cap g_2H$. Aim: $g_1H = g_2H$
  Then there are h_1, $h_2 \in H$ with $g = g_1h_1 = g_2h_2$,
  so $g_2^{-1}g_1 = h_2h_1^{-1} \in H$,
  so by the coset equality test we have $g_1H = g_2H$.
  So $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$.

This proves the first claim.

Claim. Each left coset of H has the same size as H.

Proof of claim Take $g \in G$. Define

$$\begin{aligned} f : H &\to gH \\ h &\mapsto gh. \end{aligned}$$

This is a bijection (it has inverse $\tilde{g} \mapsto g^{-1}\tilde{g}$).

So $|H| = |gH|$.

This proves the second claim.

Then $|G| = |G/H| \times |H|$, so $|H| \mid |G|$.

□

Remark. We can define a relation $\sim$ on G via $g_1 \sim g_2$ if and only if $g_2^{-1}g_1 \in H$. We can check that $\sim$ is an equivalence relation on G, and that the equivalence classes are precisely the left cosets of H in G. This gives an alternative proof that the cosets partition G.

WARNING There is not a converse to Lagrange's Theorem. It is not in general true that if $k \mid |G|$ then G has a subgroup of order k.

For example, $|A_4| = \frac{1}{2} \times 4! = 12$, but A_4 has no subgroup of order 6 (exercise: check this).

Example. Since 13 is prime, the only subgroups of $(\mathbb{Z}_{13}, +)$ are $\{\overline{0}\}$ and $\mathbb{Z}_{13}$.

Lemma 35. *Let G be a finite group. Take $g \in G$. Then g has finite order.*

Proof. Consider g, g^2, g^3, ... These are all in the finite set G, and so there are positive integers r and s with $r < s$ and $g^r = g^s$. Then $e = g^{s-r}$, so the order of g is finite (and is at most $s - r$). □

Corollary 36. *Let G be a finite group. Take $g \in G$. Then $o(g) \mid |G|$.*

"the order of an element divides the order of the group"

Proof. Note that $\langle g \rangle = \{e, g, g^2, \ldots, g^{o(g)-1}\}$ is a subgroup of G with order $o(g)$. Now apply Lagrange. □

Corollary 37. *Let p be prime. Let G be a finite group with order p. Then G is cyclic.*

Proof. Take $g \in G \setminus \{e\}$. Then $o(g)$ divides p and is not 1, so $o(g) = p$. So g is a generator of G. □

Remark. This proof shows that any non-identity element generates G.

Corollary 38. *Let G be a finite group. Take $g \in G$. Then $g^{|G|} = e$.*

Proof. We have $g^{o(g)} = e$ and $o(g) \mid |G|$. □

The next theorem is another corollary of Lagrange's Theorem.

Theorem 39 (Fermat's Little Theorem)**.** *Let p be prime. Let a be an integer coprime to p. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. $(\mathbb{Z}_p^\times, \times)$ is a group of order $p-1$. Apply Corollary 38. □

Theorem 40 (Fermat-Euler Theorem)**.** *Let $n \geq 2$ be an integer. Let a be an integer coprime to n. Define the* Euler totient function ϕ *via*

$$\phi(n) := |\{k \in \mathbb{N} : 1 \leq k \leq n, \mathrm{hcf}(k, n) = 1\}|.$$

Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. $(\mathbb{Z}_n^\times, \times)$ is a group of order $\phi(n)$. Apply Corollary 38. □

Remark. The Euler totient function ϕ has many interesting properties. One special case is that if p is prime, then $\phi(p) = p-1$, so Fermat's Little Theorem is a special case of the Fermat-Euler theorem.

7 Historical interlude

On MacTutor, you will find two short outlines of the historical development of the idea of a group, one at `http://mathshistory.st-andrews.ac.uk/HistTopics/Development_group_theory.html` and another at `http://mathshistory.st-andrews.ac.uk/HistTopics/Abstract_groups.html`. It's an interesting story, and well worth exploring to trace the development of a mathematical concept.

Why is the Chinese Remainder Theorem so named? The first known instance of the sort of problem (which we would now express using simultaneous congruences) that can be solved using this approach is in a Chinese text called *Sunzi suanjing*, by Sun Zi, probably written around the 5th century CE. For more discussion of this work, and the date it was written, you could consult `http://mathshistory.st-andrews.ac.uk/Biographies/Sun_Zi.html` . As with other ideas in maths, this one was refined and developed further by others, including for example Qin Jiushao (see below).

The MacTutor website has biographies of many mathematicians. Here are some whose names have occurred in this course, or who are in other ways importantly connected with the study of abstract algebra (which includes group theory).

- Niels Abel (1802–1829) http://mathshistory.st-andrews.ac.uk/Biographies/Abel.html
- Augustin-Louis Cauchy (1789–1857) http://mathshistory.st-andrews.ac.uk/Biographies/Cauchy.html
- Arthur Cayley (1821–1895) http://mathshistory.st-andrews.ac.uk/Biographies/Cayley.html
- Leonhard Euler (1707–1783) http://mathshistory.st-andrews.ac.uk/Biographies/Euler.html
- Pierre de Fermat (1601–1665) http://mathshistory.st-andrews.ac.uk/Biographies/Fermat.html
- Évariste Galois (1811–1832) http://mathshistory.st-andrews.ac.uk/Biographies/Galois.html
- Qin Jiushao (1202–1261) http://mathshistory.st-andrews.ac.uk/Biographies/Qin_Jiushao.html
- Joseph-Louis Lagrange (1736–1813) http://mathshistory.st-andrews.ac.uk/Biographies/Lagrange.html
- Emmy Noether (1882–1935) http://mathshistory.st-andrews.ac.uk/Biographies/Noether_Emmy.html
- Sun Zi (about 400 to about 460) http://mathshistory.st-andrews.ac.uk/Biographies/Sun_Zi.html

The Groups and Groups Actions course will continue in Trinity Term!