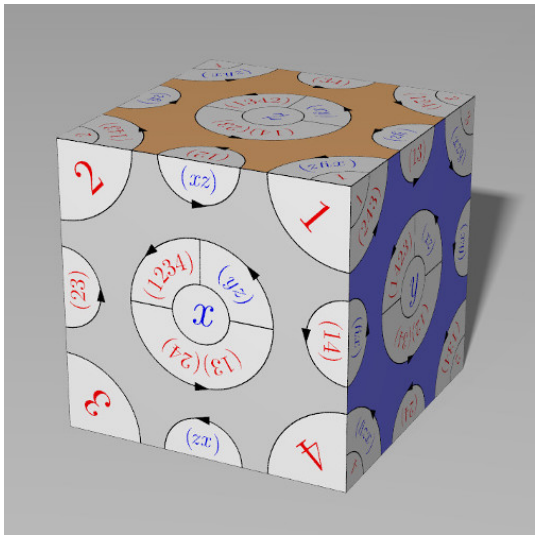
Ia Groups

Julia Goedecke (jg352)



Contents

Preamble

The Notes

These notes are *not* verbatim what I will write in the lectures, but the content is exactly the same. The main difference is that they have more complete sentences, and they may have some comments that I only said in lectures. I might try to make such comments green, but it may not be consistent.

If you find any errors and typos in the notes, please do let me know (jg352), even if they look trivial.

How to use the notes

You can read ahead of lectures, you can use them for revision, you can use them to look up a little detail which you can't figure out from your copy of the lectures, and probably in many more ways. It is up to you to find out how they are most useful. If you don't like taking notes at all in lectures, use these. If you (like me) find that taking down notes in lectures is actually the best way to learn something, set these notes aside for a while and use them just to fill in gaps later. If you try to read these notes while I'm lecturing the same material, you may get confused and probably won't hear what I say. So my advice is to follow one of these three possibilities: take notes in lectures; read ahead and then listen in lectures knowing you've already seen it in the notes; listen in lectures hoping that it will all be written in the notes.

How to treat references in the notes

There are two types of references: referring back to something we've already done, or referring forward to something that we will do later in this course, or you will do later in a different course. The first kind are obvious: if we need to use a result or example, we like to be able to look back to remember all the details. The second kind you can ignore on first reading if you like. They are meant to put things in context and whet your appetite for more maths :-). You might be interested in them later, for example when you revise the course or learn more in other courses. Think of them as cross-references.

All references to places inside the text are hyperlinked for your convenience.

Exercises

Sometimes in the notes I will say "exercise". The main reason to have these is for you to be able to check your understanding by doing a fairly straight-forward exercise yourself. Example sheet questions usually go a bit further and require thinking, whereas such exercises in the text should be easy if you're comfortable with the material, and a good starting point to get comfortable with the material if you are not quite yet.

Blog

You will find summaries, some suggestions for understanding, and some links to interesting material outside the course on my course blog. `juliagoedecke.wordpress.com`

CHAPTER 1

Groups and Homomorphisms

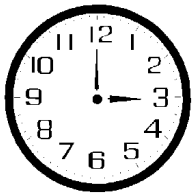
Addition modulo 3

(or any whole number n).

An example of modular arithmetic is reading the clock. For whole numbers x, y and n we write

$$x \equiv y \pmod{n} \qquad \Leftrightarrow \qquad (x-y) = kn \quad \text{for some whole number } k.$$

So, we treat two numbers as "the same" (or *congruent*) modulo n if we can subtract or add a multiple of n from the first number to get the second number. We could imagine it more easily on a clock: when we have reached n, we start again at 0. So the only important numbers are really the numbers from 0 to $n-1$ (because we can always reach one of these through addition or subtraction of n). We can write into a table how we add these numbers (see below).



Addition modulo 3

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We only really use the numbers $0, \ldots, n-1$.

If we compare usual addition with this addition mod n, we might come up with the following properties:

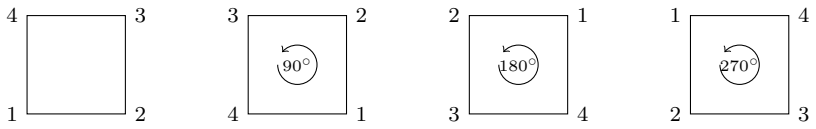
- ◇ adding two numbers gives another number between $0, \ldots, n-1$.
- ◇ 0+something = the same something ($0 + a = a$).
- ◇ We can always find a number to add that will give 0 as result.
- ◇ It does not matter how we set brackets.
- ◇ The order of adding numbers doesn't matter.

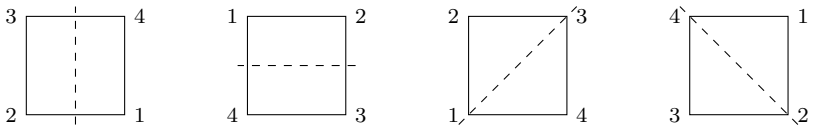
Symmetries of a square

As a second example we will look at symmetries of a square.

First we have to be clear about the meaning of the word *symmetry*. What we mean by this is a mapping of a geometrical object which sends the object onto itself. That is, the object looks the same afterwards (though the numbers of the corners may have changed).

Let's just draw all symmetries of a square that we can think of.





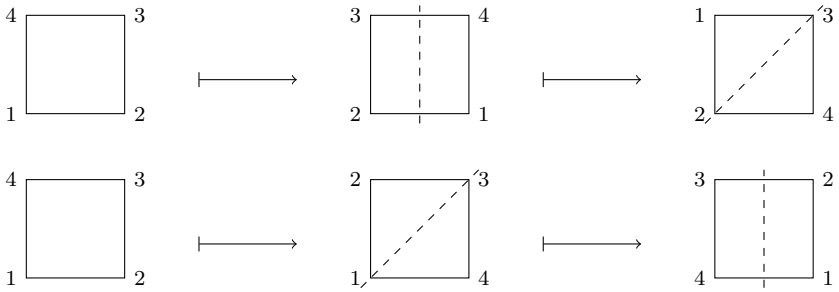
So we see there are two different kinds of symmetries: rotations and reflections. We will count the rotation angle anti-clockwise (that is just a convention). But how do we know we have written down all symmetries? Perhaps we missed some!

We can argue this way: if we take the corner labelled 1, we can map it to one of four corners. Once we have decided that, the corner labelled 2 has to go to a corner next to where we mapped 1, so there are two possibilities. Once we have decided that as well, everything else is fixed and we have no further choices. So we see that we should get $4 \cdot 2 = 8$ different symmetries, and we have indeed listed them all.

Remember this and compare when we do group actions in Chapter 5, Section Orbits and Stabilisers.

Properties:

- ◇ doing two symmetries after another gives another.
- ◇ "do nothing" before or after a symmetry doesn't change it.
- ◇ For each symmetry, there is one that "undoes" it.
- ◇ It does not matter how we set brackets. (Harder here: try examples yourself.)
- ◇ Does the order matter? It does!



As you can see, these give different answers: the top combination gives rotation by 270°, and the bottom combination gives 90° rotation.

We will use these common properties to define an abstract structure which we can work with instead of these specific examples. For that we need to know:

An **operation** is a way of combining two elements to get a new element.

For example, $n + m$ in $\mathbb{Z}$, or $a +_3 b \pmod 3$, or $v \circ r$ (composition).

[More formally: it is a function $X \times X \longrightarrow X$. Come back to this when you've done functions.]

Group axioms

Definition: A **group** is a set G with an operation $*$ satisfying the following axioms:

0. for all $a, b \in G$, we have $a * b \in G$; (**closure**)
1. there is $e \in G$ such that for all $a \in G$, $a * e = a = e * a$; (**identity**)
2. for each $a \in G$ there is $a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$; (**inverses**)
3. for all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$. (**associativity**)

If we also have

4. for all $a, b \in G$, $a * b = b * a$, (**commutativity**)

then the group is called **abelian**.

[Strictly speaking we have to say "there exists e such that all of these axioms hold".]

Examples: a) Integers $\mathbb{Z}$ with $+$ form a group.

b) Rationals $\mathbb{Q}$ with $+$ form a group.

c) $\mathbb{Z}_n$, intergers mod n, with $+_n$ form a group.
d) $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ with $\cdot$ form a group. [Check all the axioms: Practice Sheet A]
e) $\{1, -1\}$ with $\cdot$ forms a group:

$\cdot$	1	-1
1	1	-1
-1	-1	1

f) Symmetries of a regular triangle with composition form a group. We can use any regular n-gon: c.f. dihedral group D_{2n} later, e.g. D_8 is group of symmetries of square.
g) 2×2 invertible matrices with matrix multiplication form a group. [Check all the axioms.] This group is called $\mathrm{GL}_2(\mathbb{R})$ (see Chapter 8).
h) Symmetry groups of 3-dimensional objects such as cube, terahedron, toblerone box, ... under composition.

Which of these are abelian groups?

Counterexamples:
a) $\mathbb{Z}$ with $\cdot$: what is the inverse of 3? Axiom 2 fails.
b) $\mathbb{Q}$ with $\cdot$: what is the inverse of 0? Axiom 2 fails.
c) $\mathbb{Z}_4\backslash\{0\}$ with $\cdot_4$: what is $2 \cdot_4 2$? Axiom 0 fails.
d) $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ with division: Can you find an identity Axiom 1 fails.
e) $\mathbb{Z}$ with $-$: is $(3-4)-2$ the same as $3-(4-2)$? Axiom 3 fails.
f) $\mathbb{Z}$ with "to the power of": $(2^3)^2 = 8^2 = 64$ but $2^{(3^2)} = 2^9 = 512$. Axiom 3 fails.

[Look at examples and counterexamples on the Practice Sheets.]

Some simple properties

1 Proposition: *Let $(G, *)$ be a group. Then*
(i) The identity is unique.
(ii) Inverses are unique.

PROOF. (i) Suppose both e and e' are identities in G. Then $e*e' = e'$ as e is an identity, and $e * e' = e$ as e' is an identity. So $e = e'$.
(ii) Suppose both a^{-1} and b satisfy Axiom 2 for $a \in G$. Then $b = b*e = b*(a*a^{-1}) = (b*a)*a^{-1} = e*a^{-1} = a^{-1}$. Here we are using in order: Axiom 1, Axiom 2, Axiom 3, Axiom 2, Axiom 1.

□

2 Proposition: *Let $(G, *)$ be a group, and let $a, b \in G$. Then*
(i) $(a^{-1})^{-1} = a$ *"a is the inverse of its inverse."*
(ii) $(a*b)^{-1} = b^{-1}*a^{-1}$ *"socks and shoes".*

PROOF. (i) Given a^{-1}, both a and $(a^{-1})^{-1}$ satisfy $x*a^{-1} = e = a^{-1}*x$, so by uniqueness of inverses, $a = (a^{-1})^{-1}$.
(ii) $(a*b)*(b^{-1}*a^{-1}) = a*(b*(b^{-1}*a^{-1})) = a*((b*b^{-1})*a^{-1}) = a*(e*a^{-1}) = a*a^{-1} = e$. Similarly $(b^{-1}*a^{-1})*(a*b) = e$, so by uniqueness of inverses, $(a*b)^{-1} = b^{-1}*a^{-1}$.

□

Remarks:
◇ From now on we will use that "Associativity means we can leave out brackets". c.f. Practice Sheet B Q3.
◇ If clear from context, we leave out $*$: e.g. $(ab)^{-1} = b^{-1}a^{-1}$.
◇ We often just write G instead of $(G, *)$ if the operation is clear.

Definition: A group $(G, *)$ is a **finite group** if the set G has finitely many elements. Then the **order** of G is $|G|$, the number of elements of G.

Exercise: Which of our examples are finite groups?

Subgroups

Let $(G, *)$ be a group throughout.

Definition: A **subgroup** $(H, *) \leqslant (G, *)$ (or $H \leqslant G$) is a subset $H \subseteq G$ such that H with the restricted operation $*$ from G is also a group. If $H \leqslant G$ and $H \neq G$, we call H a **proper** subgroup.

Examples: a) $(\mathbb{Z}, +) \leqslant (\mathbb{Q}, +) \leqslant (\mathbb{R}, +) \leqslant (\mathbb{C}, +)$
b) We always have $(\{e\}, *) \leqslant (G, *)$ (trivial subgroup) and $(G, *) \leqslant (G, *)$.
c) $(\{1, -1\}, \cdot) \leqslant (\mathbb{Q}^*, \cdot)$.

3 Lemma: ("Usual subgroup criterion")
Let $(G, *)$ be a group and let $H \subseteq G$ be a subset. Then $H \leqslant G$ if and only if
(i) $e \in H$, and *"identity is in H"*
(ii) for $a, b \in H$, also $a * b \in H$, and *"closed under $*$"*
(iii) for $a \in H$, also $a^{-1} \in H$. *"closed under inverses"*

Proof. We have to use the group axioms 0.–3., applied to H. First note that associativity in H is inherited from G, meaning Axiom 3 holds in H as soon as it holds in G. (So we don't have to check it.)

Clearly (i) ⇒ Axiom 1, (ii) ⇒ Axiom 0 and (iii) ⇒ Axiom 2.

Conversely, suppose $(H, *)$ is also a group. Does e_H have to be the same as the identity $e \in G$? Yes: $e_H * e_H = e_H$ in H, so also in G. In G, e_H has some inverse, so $e_H * e_H * e_H^{-1} = e_H * e_H^{-1}$, which gives $e_H = e$. So Axiom 1 ⇒ (i). Also Axiom 2 ⇒ (iii) by uniqueness of inverses in G, and Axiom 0 ⇒ (ii) easily. □

Examples: d) The rotations of a square form a subgroup of D_8 (all symmetries of the square). Check: (i) clearly true, (ii) two rotations give another rotation, (iii) inverse is the rotation in the opposite direction (or $360^\circ -$ first rotation).
e) Even numbers form a subgroup of the integers: $2\mathbb{Z} \leqslant \mathbb{Z}$. (i) 0 is even, (ii) $2a+2b = 2(a+b)$, (iii) $-2a = 2(-a)$.

4 Lemma: ("Super-efficient subgroup criterion")
Let $(G, *)$ be a group and $H \subseteq G$. Then $(H, *) \leqslant (G, *)$ if and only if
I. H is not empty and
II. given $a, b \in H$, also $a * b^{-1} \in H$.

Proof. "⇒" If H is a subgroup, then $e \in H$, so H is not empty. Combining closure under inverses and multiplication gives II.

"⇐" We show conditions (i), (ii), (iii) of the usual subgroup criterion (Lemma 3). By I, there is some $h \in H$, so using II on h, h we get $e = h * h^{-1} \in H$. Now for all $a \in H$, use II on e, a to get $e * a^{-1} = a^{-1} \in H$. Finally, for $a, b \in H$, we have just shown that $b^{-1} \in H$, so use II on a, b^{-1} to get $a * b = a * (b^{-1})^{-1} \in H$. □

5 Proposition: ("subgroups of $\mathbb{Z}$")
The subgroups of $(\mathbb{Z}, +)$ are exactly $n\mathbb{Z}$ for $n \in \mathbb{Z}$.

Proof. For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a subgroup: $0 \in n\mathbb{Z}$, and for $a, b \in n\mathbb{Z}$, we have $a = na', b = nb'$ for $a', b' \in \mathbb{Z}$, so $a - b = n(a' - b') \in n\mathbb{Z}$, so by the super-efficient subgroup criterion (Lemma 4), $n\mathbb{Z}$ is a subgroup.

Conversely, let $H \leqslant \mathbb{Z}$. We know $0 \in H$. If $H = \{0\}$, it is $0\mathbb{Z}$. Otherwise pick n to be the smallest positive integer in H. We show $H = n\mathbb{Z}$. Suppose $a \in H$ is not divisible by n, so $a = nk + a'$, with $a' \in \{1, \ldots, n-1\}$. But as H is a subgroup, $nk = n + n + n + \ldots + n \in H$,

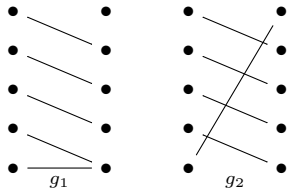
so $a - nk = a' \in H$, contradicting the fact that n is the *smallest* positive integer in H. So every $a \in H$ is divisible by n, i.e. $H = n\mathbb{Z}$. □

Small detour about functions

You'll do this also in N+S.

Given two sets X and Y, a **function** $f\colon X \longrightarrow Y$ sends each $x \in X$ to a particular $f(x) \in Y$. X is the **domain** or **source**, Y is the **codomain** or **target** of f.

Examples:
- $1_X\colon X \longrightarrow X$ with $1_X(x) = x$ — **identity function** (sometimes written id)
- $\iota\colon \mathbb{Z} \longrightarrow \mathbb{Q}$ with $\iota(n) = n$ — **inclusion map**
- $f_1\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ with $f_1(n) = n + 1$
- $f_2\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ with $f_2(n) = 2n$
- $f_3\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ with $f_3(n) = n^2$
- $g_1\colon \{0,1,2,3,4\} \longrightarrow \{0,1,2,3,4\}$ with $g_1(x) = x + 1$ if $x < 4$, $g_1(4) = 4$.
- $g_2\colon \{0,1,2,3,4\} \longrightarrow \{0,1,2,3,4\}$ with $g_2(x) = x + 1$ if $x < 4$, $g_2(4) = 0$.



Functions can be **composed** (applied one after another): if $f\colon X \longrightarrow Y$ and $g\colon Y \longrightarrow Z$, then $g{\circ}f\colon X \longrightarrow Z$ is defined by $g{\circ}f(x) = g(f(x))$. For example, from above: $f_2{\circ}f_1(n) = 2n + 2$, $f_1{\circ}f_2(n) = 2n + 1$.

Two functions f, g are **the same** ($f = g$) if they have the same source X and same target Y, and for all $x \in X$ we have $f(x) = g(x)$.

A function f is **injective** if it "hits everything at most once": if $f(x) = f(y)$ then $x = y$. A function f is **surjective** (or onto) if it "hits everything at least once": for all $y \in Y$ there is $x \in X$ with $f(x) = y$. A function $f\colon X \longrightarrow Y$ is **bijective** if it is injective and surjective (i.e. it "hits everything exactly once").

Examples: ι and f_2 are injective but not surjective. f_3 and g_1 are neither, 1_X, f_1 and g_2 are bijective.

Bijective functions $f\colon X \longrightarrow Y$ have inverses: $f^{-1}\colon Y \longrightarrow X$ with $f{\circ}f^{-1} = 1_Y$ and $f^{-1}{\circ}f = 1_X$.

Exercise: Write down the inverses to 1_X, f_1 and g_2. If X is a finite set, prove $f\colon X \longrightarrow X$ is surjective if and only if it is injective.

6 Lemma: *The composite of bijective functions is bijective.*

Proof. Exercise or see N+S. □

Group homomorphisms

We are interested in functions/maps that "preserve" or "respect" the group operation.

Definition: Let $(G, *)$ and $(H, \star)$ be groups. Then $f\colon G \longrightarrow H$ is a **group homomorphism** (or just **homomorphism**) if for all $a, b \in G$ we have $f(a * b) = f(a) \star f(b)$.

In words: It does not matter if we first multiply in G and then send the answer to H, or first send each element to H and then multiply them there.

Definition: A homomorphism that is also a bijective function is an **isomorphism**.

Examples: a) $1_G\colon G \longrightarrow G$ and $\iota\colon \mathbb{Z} \longrightarrow \mathbb{Q}$ are group homomorphisms. So is $f_2\colon \mathbb{Z} \longrightarrow \mathbb{Z}$. The other previous examples are not (find out why). Which of the above are isomorphisms?

b) $\exp\colon (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$ with $\exp(x) = e^x$ is a group homomorphism:

$$\exp(x+y) = e^{x+y} = e^x e^y = \exp(x)\exp(y)$$

Is it injective? Surjective? What about $\exp\colon (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \cdot)$?

c) Take $(\mathbb{Z}_4, +_4)$ and $H = \{1, e^{i\frac{\pi}{2}}, e^{i\pi}, e^{i\frac{3\pi}{2}}\}$ with complex multiplication (4th roots of unity). Define $f\colon \mathbb{Z}_4 \longrightarrow H$ by $f(a) = e^{i\frac{a\pi}{2}}$. Excercise: Show this is an isomorphism (i.e. a bijective group homomorphism).

d) $f\colon \mathrm{GL}_2(\mathbb{R}) \longrightarrow \mathbb{R}^*$ with $f(A) = \det A$ is a homomorphism: $\det(AB) = \det A \det B$.

Definition: Two groups are called **isomorphic** if there is an isomorphism between them. We write $G \cong H$ and think of them as "the same" group.

7 Proposition: ("Properties of group homs")

(i) Group homomorphisms send the identity to the identity: $f(e) = e$.
(ii) Group homomorphisms send inverses to inverses: $f(a^{-1}) = f(a)^{-1}$.
(iii) The composite of two group homomorphisms is a group homomorphism.
(iv) The composite of two isomorphisms is an isomorphism.
(v) The inverse of an isomorphism is an isomorphism.

Proof. (i) Let $f\colon (G, *) \longrightarrow (H, \star)$ be a group homomorphism. Then we have $f(e_G) = f(e_G * e_G) = f(e_G) \star f(e_G)$. Now $f(e_G) \in H$ has an inverse, so multiplying by this we get:

$$\begin{aligned} f(e_G)^{-1} \star f(e_G) &= f(e_G)^{-1} \star f(e_G) \star f(e_G) \\ \Leftrightarrow e_H &= f(e_G). \end{aligned}$$

(ii) Exercise.

(iii) Let $f\colon G_1 \longrightarrow G_2$ and $G\colon G_2 \longrightarrow G_3$ be group homomorphisms. Then for $a, b \in G_1$, we have

$$\begin{aligned} g\circ f(a *_1 b) = g(f(a *_1 b)) &= g(f(a) *_2 f(b)) && \text{as } f \text{ is group homomorphism} \\ &= g(f(a)) *_3 g(f(b)) && \text{as } g \text{ is group homomorphism} \\ &= g\circ f(a) *_3 g\circ f(b). \end{aligned}$$

(iv) Combine (iii) and Lemma 6: the composite of bijective group homomorphisms is still a group homomorphism and bijective.

(v) Let $f\colon G \longrightarrow H$ be an isomorphism. So it is a bijection and has an inverse function $f^{-1}\colon H \longrightarrow G$. We show that f^{-1} is also a group homomorphism (and so an isomorphism, as it is bijective).

Take $x, y \in H$. Then there are $a, b \in G$ with $f(a) = x$ and $f(b) = y$ because f is bijective. Then $f^{-1}(x * y) = f^{-1}(f(a) * f(b)) = f^{-1}(f(a * b)) = a * b = f^{-1}(x) * f^{-1}(y)$. □

Images and Kernels

Definition: If $f\colon G \longrightarrow H$ is a group homomorphis, then the **image of** f

$$\mathrm{Im} f = \{b \in H \mid \exists a \in G \text{ s.t. } f(a) = b\} = \text{"}f(G)\text{"} = \{f(a) \mid a \in G\}$$

is the set of elements in H "hit by f";

and the **kernel of** f

$$\operatorname{Ker} f = \{a \in G \mid f(a) = e_H\} = \text{“}f^{-1}(\{e_H\})\text{”}$$

is the set of elements in G which are mapped to the identity (the *preimage* of $\{e_H\}$).

8 Proposition: (“kernels and images are subgroups”)
Let $f\colon G \longrightarrow H$ be a group homomorphism. Then the image is a subgroup of H and the kernel is a subgroup of G. In symbols: $\operatorname{Im} f \leqslant H$, $\operatorname{Ker} f \leqslant G$.

Proof. We use the “super-efficient subgroup criterion” (Lemma 4) and “properties of group homs” (Proposition 7).

I. $\operatorname{Im} f$ is not empty, as $f(e) = e$, so $e_H \in \operatorname{Im} f$. Similarly $e_G \in \operatorname{Ker} f$.

II. If $b_1, b_2 \in \operatorname{Im} f$, then there exist $a_1, a_2 \in G$ with $f(a_i) = b_i$. So

$$f(a_1 * a_2^{-1}) = f(a_1) * f(a_2)^{-1} = b_1 * b_2^{-1} \in \operatorname{Im} f.$$

II for kernel: Exercise.

□

In fact, kernels are special subgroups:
Given $f\colon G \longrightarrow H$, $a \in G$, $k \in \operatorname{Ker} f$, we have $f(a * k * a^{-1}) = f(a) * f(k) * f(a)^{-1} = f(a) * e * f(a)^{-1} = e$, so $a * k * a^{-1} \in \operatorname{Ker} f$ also. Subgroups with this property are called **normal** subgroups: see later (beginning of Chapter 4).

Examples:
a) The identity $1_G\colon G \longrightarrow G$ has image $\operatorname{Im} 1_G = G$ and kernel $\operatorname{Ker} 1_G = \{e\}$. The inclusion map $\iota\colon \mathbb{Z} \longrightarrow \mathbb{Q}$ has $\operatorname{Im}\iota = \mathbb{Z}$ and $\operatorname{Ker}\iota = \{e\}$. The map $f_2\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ with $f_2(n) = 2n$ has $\operatorname{Im} f_2 = 2\mathbb{Z}$ and $\operatorname{Ker} f_2 = \{e\}$.
b) The exponential map $\exp\colon (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$ has $\operatorname{Im}(\exp) = \mathbb{R}^+$ and $\operatorname{Ker}(\exp) = \{0\}$.
c) The homomorphism $f\colon \mathbb{Z}_4 \longrightarrow H$ as previously defined has $\operatorname{Im} f = H$ and $\operatorname{Ker} f = \{1\}$.
d) The determinant homomorphism $\det\colon \mathrm{GL}_2(\mathbb{R}) \longrightarrow (\mathbb{R}^*, \cdot)$ has $\operatorname{Im}(\det) = \mathbb{R}^*$ and kernel $\operatorname{Ker}(\det) = \{\text{all matrices with determinant } 1\} = \mathrm{SL}_2(\mathbb{R})$. (see later, Chapter 8 Matrix groups)

This suggests some relationship between images and kernels on the one hand and injectivity and surjectivity on the other hand.

9 Proposition: (“injectivity via kernels”)
A group homomorphism $f\colon G \longrightarrow H$ is
(i) surjective if and only if $\operatorname{Im} f = H$
(ii) injective if and only if $\operatorname{Ker} f = \{e\}$.

Proof. (i) Clear by definition.
(ii) “⇒” $f(e) = e$, so if $k \in \operatorname{Ker} f$, then $f(k) = e$, and so $k = e$.
“⇐” Given a, b s.t. $f(a) = f(b)$, then $f(ab^{-1}) = e$, so $ab^{-1} = e$, so $a = b$.

□

Cyclic groups

Notation: Write $a^2 = a * a$, $a^n = a * \cdots * a$ (n factors of a), $a^0 = e$, $a^{-n} = (a^{-1})^n = (a^n)^{-1}$.

Definition: A group $(G, *)$ is **cyclic** if there is an element $a \in G$ such that all elements of G are powers of a. Such an a is called a **generator**.

Examples:
a) $(\mathbb{Z}, +)$ is cyclic, with generator 1 or -1. Generators are not unique. This is “the infinite cyclic group” ⟶ cf “essential uniqueness of cyclic groups” (Lemma 39 in Chapter 4).
b) $\{+1, -1\}$ with $\cdot$ is cyclic with generator -1.

c) $(\mathbb{Z}_n, +_n)$ (integers mod n) is cyclic. 1 is a generator, but there are several other generators, depending on n.
   $n = 3$: $1, 2$ are generators ("$2 \equiv -1$")
   $n = 4$: $1, 3$ are generators ("$3 \equiv -1$")
   $n = 5$: $1, 2, 3, 4$ are generators.
d) Rotations of triangle: cyclic generated by rotation of 120° or 240°.

Notation: Given a group G and $a \in G$, we write $\langle a \rangle$ for the **cyclic subgroup generated by** a, which is defined to be the smallest subgroup containing a.

Remark: The subgroup generated by a is in fact the set of all powers of a. To see this, we first check that the set of all powers of a is a subgroup:

I. $e = a^0$ is a power of a, so the set is non-empty.
II. Given a^m, a^n, then a^{m-n} is also a power of a,

so by the super-efficient subgroup criterion, the set of power of a is a subgroup of G.

Now if a is in any subgroup, then by closure $a * a = a^2$ is in the subgroup as well, and so by induction all positive powers of a. But the inverse a^{-1} is also in the subgroup, so also all negative powers of a. So the set of powers of a is the smallest subgroup containing a.

So $\langle a \rangle$ is a subgroup by definition, we don't have to prove that. We did have to prove that it is the same as the set of powers of a, but now we can use that as well since we've proved it.

Definition: The **order** of an element $a \in G$ is the smallest positive $k \in \mathbb{N}$ s.t. $a^k = e$. If no such k exists, then a as infinite order. Write $\text{ord}(a)$ for the order of a.

10 Lemma: ("The order is the size of the cyclic subgroup.")
For $a \in G$, $\text{ord}(a) = |\langle a \rangle|$.

PROOF. If $\text{ord}(a) = \infty$, then $a^n \neq e$ for any $n \in \mathbb{Z}$, so $a^n \neq a^m$ for all $n \neq m$. Therefore $\langle a \rangle$ has infinite order.

If $\text{ord}(a) = k < \infty$, then $a^k = e$, so $\langle a \rangle = \{a^0 = e, a, a^2, \ldots, a^{k-1}\}$ because $a^k = e = a^0$, $a^{k+1} = a$, etc, and $a^{-1} = a^{k-1}$ etc. So $|\langle a \rangle| = k$. □

We write C_n for "the" cyclic group of order n (in multiplicative notation). So e.g. $C_n \cong (\mathbb{Z}_n, +)$. c.f. Lemma 39 Section The Isomorphism Theorem, Chapter 4.

Examples:
- ◇ Every element in $\mathbb{Z}$ (other than 0) has infinite order.
- ◇ $1 \in \mathbb{Z}_n$ has order n.
- ◇ $e \in G$ always has order 1.

11 Proposition: *Cyclic groups are abelian.*

PROOF. Exercise. □

Remark: Let G be a group, $a_1, \ldots, a_k \in G$. Then $\langle a_1, \ldots, a_k \rangle$ is the subgroup generated by $a_1, \ldots, a_k$, the smallest subgroup of G containing all a_i.

Exercise: Any subgroup of a cyclic group is cyclic.

Dihedral groups

Recall the symmetries of a regular n-gon. There are n rotations and n reflections. The rotations are generated by the rotation of $\frac{360}{n}^\circ$, let us call it r. This has order n. Any reflection has order 2. Choose your favourite one, and call it s. In fact, r and s generate the whole group of symmetries.

Dihedral group $D_{2n} = \langle r, s \mid r^n = e = s^2, srs^{-1} = r^{-1} \rangle$
(or $sr = r^{-1}s$ instead of the last relation). [This is of the form ⟨generators | relations⟩.]

As a set, $D_{2n} = \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$. Here we use for example $sr = r^{-1}s = r^{n-1}s$, $sr^k = r^{-k}s = r^{n-k}s$.

It is useful to have both the geometric viewpoint as symmetries or a regular n-gon and the algebraic viewpoint with generators and relations.

Exercise: Show that each sr^k has order 2. (These are the reflections).

Cartesian products of groups

Given two groups $(G_1, *_1)$, $(G_2, *_2)$, we can define a group operation on the set $G_1 \times G_2 = \{(a_1, a_2) \mid a_i \in G_i\}$ (the set of ordered pairs).

Definition: The product $G_1 \times G_2$ of two groups G_1, G_2 is the group with componentwise multiplication $(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$.

Exercise: Check that it really is a group!

Examples:

$$\begin{aligned} C_2 \times C_2 &= \{(e,e), (a,e), (e,b), (a,b)\} \\ &\cong \{\ e, \quad x, \quad y, \quad xy\} \\ &\cong \langle x, y \mid x^2 = y^2 = e, xy = yx \rangle \end{aligned}$$

Clearly $(a, e) * (e, b) = (e, b) * (a, e)$. All elements have order 2.

$$\begin{aligned} C_2 \times C_3 &= \{(e,e), (a,e), (e,b), (a,b), (e,b^2), (a,b^2)\} \\ &\cong \{\ e, \quad x^3, \quad x^4, \quad x, \quad x^2, \quad x^5\} \\ &\cong C_6 \end{aligned}$$

Note that we always have $(a_1, e) * (e, a_2) = (e, a_2) * (a_1, e)$. "Everything in G_1 commutes with everything in G_2."

12 Proposition: ("products of cyclic groups")
$C_n \times C_m \cong C_{nm}$ if and only if n, m are coprime.

Proof. Let $C_n = \langle a \mid a^n = e \rangle$ and $C_m = \langle b \mid b^m = e \rangle$. We have $(a, b)^k = (a^k, b^k) = e$ if and only if $a^k = e$ *and* $b^k = e$. If n, m are coprime, this happens for the first time with $k = nm$. If n, m have a common factor l, say $n = n'l$ and $m = m'l$, then $(a, b)^{n'm'l} = (e, e)$, and so there is no element of order nm. □

CAREFUL: $D_6 \ncong C_3 \times C_2$ and $D_{2n} \ncong C_n \times C_2$!!!!! (for $n > 2$)
Because: $C_n \times C_2$ is always abelian, D_{2n} is not abelian for $n > 2$.

13 Proposition: ("Direct Product Theorem")
Let $H_1, H_2 \leqslant G$ such that
(i) $H_1 \cap H_2 = \{e\}$ — *("they intersect only in e")*
(ii) for all $a_1 \in H_1, a_2 \in H_2$, have $a_1 a_2 = a_2 a_1$ — *("H_1 and H_2 commute in G")*
(iii) for all $a \in G$, there are $a_i \in H_i$ with $a = a_1 a_2$ — *("$G = H_1 H_2$" **internal product**)*
Then $G \cong H_1 \times H_2$.

Proof. Define $f\colon H_1 \times H_2 \longrightarrow G$ by $f((a_1, a_2)) = a_1 a_2$. This is a group homomorphism: $f((a_1, a_2) * (b_1, b_2)) = f((a_1 b_1, a_2 b_2)) = a_1 b_1 a_2 b_2 = a_1 a_2 b_1 b_2 = f((a_1, a_2)) f((b_1, b_2))$ using (ii). By

(iii) f is surjective. We use (i) to show that f is injective: if $f((a_1, a_2)) = e$, then $a_1 = a_2^{-1} \in H_1 \cap H_2$. So $a_1 = e = a_2$, so $\operatorname{Ker} f = \{e_{H_1 \times H_2}\}$. So by "injectivity via kernels" (Proposition 9), f is injective. Therefore f is a bijective group homomorphism, so an isomorphism. □

CHAPTER 2

Symmetric Groups Part I

Definitions

Definition: A bijection from a set X to itself is also called a **permutation** (of X). The set of all permutations on X is Sym$X$.

14 Theorem: Sym$X$ *with composition forms a group.*

PROOF. 0. If $\sigma\colon X \longrightarrow X$ and $\tau\colon X \longrightarrow X$, then $\sigma\circ\tau\colon X \longrightarrow X$. If σ, τ are both bijections, the composite is also bijective (cf. Lemma 6). So if $\sigma, \tau \in \text{Sym}X$, also $\sigma\circ\tau \in \text{Sym}X$.

1. The identity $1_X\colon X \longrightarrow X$ is clearly a permutation, and gives the identity element.
2. Every bijection has an inverse function which is also bijective, so if $\sigma \in \text{Sym}X$ then $\sigma^{-1}\colon X \longrightarrow X$ is also in Sym$X$ and satisfies the axiom for the group inverse.
3. Composition of functions is always associative. (See Sheet A)

□

Remark: X can be an infinite set!

Definition: If X is finite, say $|X| = n$, we usually use $X = \{1, 2, \ldots, n\}$ and write Sym$X = S_n$. This is the **symmetric group of degree** n.

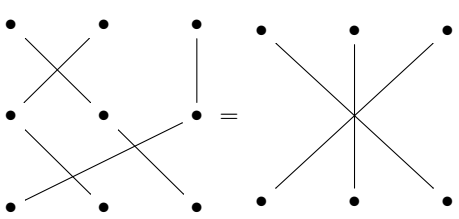
Notation: ("two row notation")

Write $1, \ldots, n$ on the top line and their images below. E.g. $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \in S_3$ or $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{bmatrix} \in S_5$. Generally, if $\sigma\colon X \longrightarrow X$, write $\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$.

Remark: Don't get too used to this notation, we'll get a better one soon.

Tricks: When composing, reorder the second element. E.g.:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

or think of strings 

Exercise: Prove that $|S_n| = n!$. (i.e. degree ≠ order)

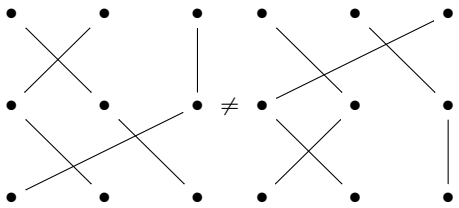
Examples: (Examples for small n)

$n = 1 \qquad S_1 = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} = \{e\} (\cong C_1)$ $\qquad\qquad$ $n = 2 \qquad S_2 = \left\{ \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \right\} \cong C_2$

$$n = 3 \qquad S_3 = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \right\}$$

Compare S_3 to the symmetries of a regular triangle, i.e. D_6. What do you find?

Exercise: Write out all subgroups of S_3. (You should get 1 of order 3, 3 of order 2, plus the trivial ones.)

Note that S_3 is not abelian: 

We can view S_3 as a subgroup of any S_n for $n \geqslant 3$: fix $4, 5, \ldots, n$.

We can also view D_{2n} as a subgroup of S_n. Take a regular n-gon and number the vertices: every symmetry of the regular n-gon is also a bijection $\{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$.

For example $D_8 \leqslant S_4$:

$$D_8 \cong \{e, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = r, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = r^2, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} = r^3, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix} = s,$$
$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} = rs, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix} = r^2 s, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = r^3 s\}$$

Here r is rotation by 90° anti-clockwise, and s is reflection in a diagonal.

Cycle notation

Example: S_3

- e — "nothing moves"
- $(123) = (231) = (312)$ — "1 goes to 2, 2 goes to 3, 3 goes to 1"
- (132)
- (12) — leave out numbers that don't move
- (13)
- (23)

Advantages: It is easy to find the order of such a cycle. (Find all orders in S_3.).
Inverses: $(123)^{-1} = (321) = (132)$. Write backwards (then cycle round to get smallest number at the front).
Composition (from right to left): $(123)(12) = (13)(2)$. Look at 1 in right-most cycle. It goes to 2. Then look at 2 in the next cycle moving to the left: there 2 goes to 3. So alltogether 1 goes to 3 and we write the 3 down. Then we look at 3. There is no 3 in the right-most cycle. In the next cycle, 3 goes to 1. We already have 1 at the beginning, so instead of writing it again we just close the bracket. Then we take the next number that we haven't written down yet, 2. In the right-most cycle, 2 goes to 1. In the next cycle, 1 goes to 2. So alltogether 2 goes to 2, so we close the bracket. This will make most sense when you see it demonstrated in lectures.

Convention: We tend to write the smallest number at the front of the cycle.

In S_4: $(12)(34)$ is one element, but (12) and (34) are also separate elements. $(1234)(14) = (1)(234)$.

Definition: We call $(a_1 a_2 \cdots a_k)$ a **k-cycle**. 2-cycles $(a_1 a_2)$ are also called **transpositions**. Two cycles are **disjoint** if no number appears in both.

Example: (12) and (34) are disjoint, but $(123), (12)$ are not, and $(123), (34)$ are not.

15 Lemma: *Disjoint cycles commute.*

PROOF. Let $\sigma, \tau \in S_n$ be disjoint cycles. We must prove: for all $a \in \{1, \ldots, n\}$, we have $\sigma(\tau(a)) = \tau(\sigma(a))$. There are three cases:

- $\diamond$ a in neither cycle is easy: $\sigma(\tau(a)) = \sigma(a) = a = \tau(a) = \tau(\sigma(a))$.
- $\diamond$ a in σ, not in τ: this means $\sigma(a) = b \neq a$, $\tau(a) = a$. Note that as σ and τ are disjoint, b is also not in the cycle τ, so also $\tau(b) = b$. Then $\sigma(\tau(a)) = \sigma(a) = b$ and $\tau(\sigma(a)) = \tau(b) = b$.
- $\diamond$ a in τ, not in σ: analogous.

□

Note that non-disjoint cycles may not commute: $(13)(23) = (132)$ but $(23)(13) = (123)$.

16 Theorem: ("disjoint cycle notation works")
For $n \geqslant 2$, every permutation in S_n can be written (essentially uniquely) as a product of disjoint cycles.

PROOF. Essentially uniquely means: the order of disjoint cycles doesn't matter, the "rotation" of individual cycles doesn't matter.

Let $\sigma \in S_n$. We start with $(1\ \sigma(1)\ \sigma^2(1)\ \sigma^3(1) \cdots)$. As $\{1, \ldots, n\}$ is finite, for some k we must have $\sigma^k(1)$ already in the list. In fact, if $\sigma^k(1) = \sigma^l(1)$ with $l < k$, then (as σ is a bijection) $\sigma^{k-l}(1) = \sigma^{l-l}(1) = 1$. So actually all $\sigma^i(1)$ are distinct until for some k we get $\sigma^k(1) = 1$ again. So the first cycle is $(1\ \sigma(1)\ \sigma^2(1)\ \cdots\ \sigma^{k-1}(1))$. Then pick the smallest (or any) number which does not appear in this cycle, say $j \in \{1, \ldots, n\} \backslash \{1, \sigma(1), \ldots, \sigma^{k-1}(1)\}$. Repeat to get the second cycle $(j\ \sigma(j)\ \cdots\ \sigma^{l-1}(j))$. As σ is a bijection, these two cycles are disjoint. We repeat until we have exhausted all $\{1, \ldots, n\}$.

Why is this essentially unique? The order of disjoint cycles doesn't matter because they commute. Any j completely determines $(j\sigma(j)\cdots)$ because σ is a function. □

We can substitute "unique" for "essentially unique" if we cycle the smallest element to the front in each cycle and then order the cycles by the size of the first number.

Look back at this proof when we've done orbits in Chapter 5, especially Lemma 43.

Definition: Writing a permuation $\sigma \in S_n$ in disjoint cycle notation, the list of cycle lengths is called the **cycle type** of σ.

Note: Of course only up to reordering. We often (but not always) leave out singleton cycles.

Examples: (12) has cycle type 2 (a transposition).
$(12)(34)$ has cycle type $2, 2$ (double transposition).
$(123)(45)$ has cycle type $3, 2$, etc.

It is easy to see that a k-cycle has order k.

17 Lemma: ("order by cycle type")
For $\sigma \in S_n$, the order of σ is the least common multiple (lcm) of the different cycle lengths in disjoint cycle notation.

PROOF. As disjoint cycles commute (Lemma 15), we can group each cycle together when taking powers: if $\sigma = \tau_1 \tau_2 \cdots \tau_l$, with the τ_i all disjoint cycles, then $\sigma^m = \tau_1^m \tau_2^m \cdots \tau_l^m$.

If cycle τ_i has length k_i, then $\tau_i^{k_i} = e$, and $\tau_i^m = e$ if and only if $k_i | m$. So to get an m such that $\sigma^m = e$, we need all k_i to divide m, i.e. we need $\text{lcm}(k_1, \ldots, k_l) | m$. So the order, which is the smallest such m, is $\text{lcm}(k_1, \ldots, k_l)$. □

Examples: Any transposition has order 2. (12)(34) also has order 2. (123)(45) has order 6.

The sign of a permutation

Permutations come in two different types: even and odd permutations. These have something in common with even and odd integers, and also something in common with positive and negative numbers.

18 Proposition: ("S_n is generated by transpositions")
Every permutation is a product of transpositions.

Proof. By disjoint cycle notation, it is enough to do this for one cycle.
$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{k-1}\ a_k)$, which is a product of $k-1$ transpositions. [Check the product.] □

We want to use this for the sign of a permutation.
BUT it is not unique, e.g.

$$(12345) = (12)(23)(34)(45) = (12)(23)(12)(34)(12)(45) = (15)(14)(13)(12) = \cdots$$

We want to find some property of such decompositions into transpositions that is invariant, i.e. only depends on the permutation we started off with.

19 Theorem: ("sign is well-defined")
Writing $\sigma \in S_n$ as a product of transpositions in different ways, σ is either always *the product of an even number of transpositions or* always *the product of an odd number of transpositions.*

Idea of proof:

- ◇ Start off with something which is determined entirely by a given permutation: number of disjoint cycles.
- ◇ Show this number changes parity when the permutation is multiplied by a transposition.
- ◇ When making a given permutation out of transpositions: the parity of "number of disjoint cycles" changes for each transposition. But end result is fixed, so parity of no of transpositions needed must be fixed.

Proof. Write $\#(\sigma)$ for the number of cycles in disjoint cycle notation, *including singleton cycles.* So $\#(e) = n$, $\#((12)) = n-1$ etc. What happens if we multiply σ by a transposition $\tau = (cd)$? (wlog $c < d$). Clearly composing with τ does not affect any cycles not containing c or d.

- ◇ If c, d are in the same σ-cycle: Say

$$(c\ a_2\ a_3\ \cdots\ a_{k-1}\ d\ a_{k+1}\ \cdots\ a_{k+l})(cd) = (c\ a_{k+1}a_{k+2}\ \cdots\ a_{k+l})(d\ a_2\ a_3\ \cdots\ a_{k-1})$$

  So $\#(\sigma\tau) = \#(\sigma) + 1$.
- ◇ If c, d are in different cycles (this could be cycles of length 1), then

$$(c\ a_2\ a_3\ \cdots\ a_{k-1})(d\ b_2 b_3\ \cdots\ b_{l-1})(cd) = (c\ b_2\ b_3\ \cdots\ b_{l-1}\ d\ a_2\ \cdots\ a_{k-1})$$

  So $\#(\sigma\tau) = \#(\sigma) - 1$.

So for any transposition τ, $\#(\sigma\tau) \equiv \#(\sigma) + 1 \pmod 2$.

Now, suppose $\sigma = \tau_1 \cdots \tau_l = \tau_1' \cdots \tau_{l'}'$ as products of transpositions. As disjoint cycle notation works (Theorem 16), $\#(\sigma)$ is completely determined by σ (i.e. it has nothing to do with these products of transpositions). But $\sigma = e\tau_1 \cdots \tau_l$, so by applying the previous result several times,

we get

$$\#(\sigma) \equiv \#(e) + l \equiv n + l \pmod 2$$
$$\text{and } \#(\sigma) \equiv \#(e) + l' \equiv n + l' \pmod 2$$

so $l \equiv l' \pmod 2$. □

Definition: Writing $\sigma \in S_n$ as a product of transpositions $\sigma = \tau_1 \cdots \tau_l$, we call $\operatorname{sgn}(\sigma) = (-1)^l$ the **sign** of σ. If $\operatorname{sgn}(\sigma) = 1$ we call σ an **even** permutation. If $\operatorname{sgn}(\sigma) = -1$ we call σ an **odd** permutation.

Note: We have proved that this is well-defined, i.e. we get the same answer no matter how we write σ as a product of transpositions.

20 Theorem: *For $n \geqslant 2$, $\operatorname{sgn}\colon S_n \longrightarrow \{\pm 1\}$ is a surjective group homomophism.*

Proof. It is a group homomorphism: $\operatorname{sgn}(\sigma_1\sigma_2) = (-1)^{l_1+l_2} = (-1)^{l_1}(-1)^{l_2} = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$, where $\sigma_1 = \tau_1 \cdots \tau_{l_1}$ and $\sigma_2 = \tau'_1 \cdots \tau'_{l_2}$ as products of transpositions.
It is surjective: $\operatorname{sgn}(e) = 1$, $\operatorname{sgn}((12)) = -1$. □

Note: The hard bit is showing that it is well-defined!!!

21 Lemma: *$\sigma \in S_n$ is an even permutation iff the number of cycles of even length is even.*

Proof. As sgn is a group homomorphism, writing σ in disjoint cycle notation $\sigma = \sigma_1 \cdots \sigma_l$, we get $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma_1) \cdots \operatorname{sgn}(\sigma_l)$. We have seen that a k-cycle is the product of $k-1$ transpositions (Proposition 18), so

$$\begin{aligned} \operatorname{sgn}(\sigma) &= (-1)^{k_1-1} \cdots (-1)^{k_l-1} \\ &= 1 && \text{iff an even number of the } k_i - 1 \text{ are odd} \\ & && \text{iff an even number of the } k_i \text{ are even} \\ (&= -1 && \text{iff an odd number of the } k_i \text{ are even}) \end{aligned}$$

□

Slogan: "odd length cycles are even, even length cycles are odd."

Definition: The kernel of $\operatorname{sgn}\colon S_n \longrightarrow \{\pm 1\}$ is called the **alternating group**: $\ker(\operatorname{sgn}) = A_n$.

Remark: As a kernel, $A_n \leqslant S_n$. [Indeed, as a kernel A_n is a *normal* subgroup of S_n, c.f. Chapter 4.]
You will meet/have met sgn in the definition of the determinant of a matrix: if A is an $n \times n$ matrix, $A = (a_{ij})$, then $\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\ \sigma(1)} \cdots a_{n\ \sigma(n)}$.

22 Proposition: *Any subgroup of S_n contains either no odd permutations, or exactly half.*

Proof. See Q3 Sheet 2. Revisit this after we've done the Isomorphism Theorem (Thm 38): that gives another way to prove this. □

CHAPTER 3

Lagrange Theorem

Cosets

Definition: Let $H \leqslant G$ and $a \in G$. The set $aH \coloneqq \{ah \mid h \in H\}$ is a **left coset** of H. Similarly $Ha \coloneqq \{ha \mid h \in H\}$ is a **right coset** of H.

Examples: a) Take $2\mathbb{Z} \leqslant \mathbb{Z}$. Then $6 + 2\mathbb{Z} = \{$ all even numbers $\} = 0 + 2\mathbb{Z}$ and $1 + 2\mathbb{Z} = \{$ all odd numbers $\} = 17 + 2\mathbb{Z}$.

b) Take $G = S_3$, $H = \langle (12) \rangle = \{e, (12)\}$. The left cosets are:

$$eH = (12)H = \{e, (12)\}; \quad (13)H = \{(13), (123)\} = (123)H; \quad (23)H = \{(23)(132)\} = (132)H$$

c) Take $G = D_6$. Recall $D_6 = \langle r, s \mid r^3 = e = s^2, rs = sr^{-1} \rangle$. Take $H = \langle s \rangle = \{e, s\}$. Then the left coset $rH = \{r, rs = sr^{-1}\}$ is not the same as the right coset $Hr = \{r, sr\}$. Try the same in S_3, and find other cosets for D_6. [Notice something?]

In the next section we are going to prove some important properties of cosets. For this we need a definition first.

Definition: Let X be a set, and $X_1, X_2, \ldots, X_n$ subsets of X. Then the X_i are called a **partition** of X if

(i) $\bigcup_{i+1}^{n} X_i = X$ ("union gives all of X") or equivalently
$\forall x \in X \exists i$ s.t. $x \in X_i$ ("every element of X is in at least one X_i")

(ii) $X_i \cap X_j = \varnothing$ for all $i \neq j$ ("pairwise disjoint") ("each element is in at most one X_i")

We will prove that the left cosets of H partition G, and that they all have the same size.
Note: We can have $aH = bH$ with $a \neq b$, see example $2\mathbb{Z} \leqslant \mathbb{Z}$.

The Theorem

23 Theorem: (Lagrange)
If G is a finite group and $H \leqslant G$, then $|H|$ divides $|G|$.

Proof. First step: we prove that the left cosets partition G.

(i) For each $a \in G$, we have $a \in aH$, so every element is in at least one coset.

(ii) We need to prove: for $a, b \in G$, the cosets aH and bH are either the same or disjoint.
Suppose aH, bH are not disjoint. So there exists some $h_1 \in H$ such that $ah_1 \in bH$ (i.e. $ah_1 \in aH \cap bH$). So $ah_1 = bh_2$ for some $h_2 \in H$. Then $a = bh_2h_1^{-1}$, so for *any* $h \in H$, we have $ah = bh_2h_1^{-1}h \in bH$. So $aH \subseteq bH$. Similarly $b = ah_1h_2^{-1}$ and $bH \subseteq aH$, so the two cosets are the same.

Second step: We prove that all left cosets have the same size (as H). Let $a \in G$. Consider

$$\begin{aligned} H &\longleftrightarrow aH \\ h &\longmapsto ah \\ a^{-1}b &\longleftarrow\!\shortmid b \end{aligned}$$

Check: These are well-defined functions, and mutually inverse. So they give a bijection between the sets H and aH.

So if $|H|$ is finite, then $|H| = |aH|$ for all $a \in G$. So putting both parts together: G is the disjoint union of distinct cosets, all of which have size $|H|$, so $|G|$ = number of cosets $\cdot\, |H|$. □

We only need $|G|$ finite in the very last step of the proof!
We could do the same proof with right cosets.

Definition: We write $|G : H|$ for the number of cosets of H in G, and call it the **index** of H in G.

So

$$|G| = |G : H||H|$$

24 Fact: ("same coset check")
$aH = bH \Leftrightarrow b^{-1}a \in H$. (see in proof: $a = bh_2h_1^{-1}$, so $b^{-1}a = h_2h_1^{-1} \in H$)

Exercise: Do the other direction.

Lagrange Corollaries

25 Corollary: ("element order divides group order")
Let G be a finite group and $a \in G$. Then $\mathrm{ord}(a) \mid |G|$.

Proof. Consider the subgroup $H = \langle a \rangle$ generated by a. We know that $\mathrm{ord}(a) = |\langle a \rangle|$, and by Lagrange $|H| \mid |G|$. □

26 Corollary: ("exponent divides group order")
Let G be a finite group. Then for each $a \in G$, $a^{|G|} = e$.

Proof. We know $|G| = \mathrm{ord}(a) \cdot k$ for some $k \in \mathbb{Z}$. So $a^{|G|} = (a^{\mathrm{ord}(a)})^k = e^k = e$. □

Recall: the **exponent** of G is the smallest number m s.t. $a^m = e$ for all $a \in G$.
We have proved the statement of the corollary, but not quite the name: it should not be too hard for you to prove the statement suggested by the name as well.

27 Corollary: ("prime order groups")
Groups of prime order are cyclic. Moreover, such groups are generated by any of their non-identity elements.

Proof. Say $|G| = p$. Let $a \in G$. If $a = e$, then $\langle a \rangle = \{e\}$. Otherwise $H = \langle a \rangle \neq \{e\}$, and $|H|$ divides $|G|$ by Lagrange. As $|G|$ is prime, $|H| = |G|$, so $\mathrm{ord}(a) = p$ and $G = \langle a \rangle$ is cylic. As the element a was arbitrary, any non-identity element generates G. □

Small detour on equivalence relations

Definition: Let X be a set. An **equivalence relation** $\sim$ on X is a relation which is
(i) **reflexive**: $x \sim x$ for all $x \in X$
(ii) **symmetric**: $x \sim y \Rightarrow y \sim x$ for all $x, y \in X$
(iii) **transitive**: If $x \sim y$ and $y \sim z$, then $x \sim z$, for all $x, y, z \in X$.

The symbol $\sim$ is officially called "tilde". It is also sometimes called "twiddle" (slightly less formally). I like the fact that you can use "twiddle" also as a verb, as in "x twiddles y".

Examples: a) $X = \mathbb{Z}$, the relation $\equiv_n$ defined as $a \equiv_n b \pmod{n} \Leftrightarrow n \mid a - b$.
b) X any set of groups, $\cong$ "isomorphic to" is an equivalence relation.
This is a hidden exercise.

Definition: Given an equivalence relation $\sim$ on X, the **equivalence classes** are

$$[x]_\sim (= [x]) = \{y \in X \mid x \sim y\}$$

28 Proposition: *Equivalence classes form a partition.*

PROOF. Let $\sim$ be an equivalence relation on the set X.
(i) Each $x \in X$ is in the class $[x]$.
(ii) If $[x] \cap [y] \neq \varnothing$, then there is some $z \in [x] \cap [y]$, i.e. $x \sim z$ and $y \sim z$. Then (using symmetry and transitivity) we can show that $x \sim y$, and any w with $x \sim w$ also satisfies $y \sim w$. So $[x] = [y]$ (because the argument is symmetric in x and y).

□

Are cosets equivalence classes for some equivalence relation? Easy answer: yes, just set $a \sim b$ iff a, b in same coset. But we will find a more interesting answer.

29 Lemma: ("coset equivalence relation")
Let $H \leqslant G$. Defining $a \sim b$ if $b^{-1}a \in H$ gives an equivalence relation on G, whose equivalence classes are the left cosets of H.

PROOF. We check the three conditions of an equivalence relation.
Reflexivity: $a^{-1}a \in H$ so $a \sim a$.
Symmetry: If $b^{-1}a \in H$ then also $(b^{-1}a)^{-1} = a^{-1}b \in H$. So $a \sim b \Rightarrow b \sim a$.
Transitivity: If $a \sim b$ and $b \sim c$, we have $b^{-1}a, c^{-1}b \in H$. So $c^{-1}bb^{-1}a = c^{-1}a \in H$, so $a \sim c$.
By "same coset check" (Fact 24), it follows that $a \sim b$ iff $aH = bH$ iff $a \in bH$ and $b \in aH$, so equivalence classes are exactly the cosets. □

Notice: the fact that the identity is inside the subgroup gives reflexivity, closure under inverses gives symmetry, and closure under group multiplication gives transitivity.
G is not necessarily finite!

Applications of Lagrange

Consider $(\mathbb{Z}, +)$ and, for fixed n, take the subgroup $H = n\mathbb{Z}$. The cosets are: $0 + H = [0]$, $1 + H = [1]$, $\ldots$, $n - 1 + H = [n - 1]$. We can call the numbers $0, \ldots, n - 1$ **representatives** of the cosets.
Calculating "mod n": Define $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$.
We need to check that these are well-defined! If $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then $a_1 = a_2 + kn$, $b_1 = b_2 + ln$ for some $k, l \in \mathbb{Z}$. So $a_1 + b_1 = a_2 + b_2 + n(k + l)$ and $a_1 \cdot b_1 = (a_2 + kn)(b_2 + ln) = a_2b_2 + n(kb_1 + la_2 + kln)$. So $[a_1 + b_1] = [a_2 + b_2]$ and $[a_1b_1] = [a_2b_2]$.
We have seen that $(\mathbb{Z}_n, +_n)$ is a group. What happens with multiplication? We can only take elements which have inverses. (called **units** → c.f. GRM in second year)
Let $U_n = \{[a] \mid a \text{ coprime to } n\}$. (We will see that these are the units.) Define the **Euler totient function** $\varphi(n) = |U_n|$. E.g. $\varphi(p) = p - 1$ for p prime, $\varphi(4) = 2$.

30 Proposition: ("mult mod n as group")
U_n is a group under multiplication mod n.

PROOF. The operation is well-defined, see above.
Closure: If a and b are coprime to n, then ab is also coprime to n. So $[a], [b] \in U_n \Rightarrow [a][b] = [ab] \in U_n$.
Identity: [1] (clearly)
Inverses: Let $[a] \in U_n$, and consider the map "multiplication by a"

$$\begin{aligned} U_n &\longrightarrow U_n \\ [c] &\longmapsto [ac] \end{aligned}$$

This is injective: if $[ac_1] = [ac_2]$, then n divides $a(c_1 - c_2)$, so as a and n are coprime, n divides $c_1 - c_2$, so $[c_1] = [c_2]$.

As U_n is finite, any injection $U_n \longrightarrow U_n$ is also a surjection (recall exercise from "small detour about functions" Chapter 1, or see N+S). So there is a c such that $[ac] = [a][c] = [1]$. So $[a]$ has an inverse in U_n.

Associativity and commutativity follow from the corresponding properties of $\mathbb{Z}$ (because the operation $[a][b] = [ab]$ is well-defined). □

31 Theorem: (Fermat-Euler)
Let $n \in \mathbb{N}$, and $a \in \mathbb{Z}$ be coprime to n. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

*In particular (**Fermat's Little Theorem**): If $n = p$ is prime, then $a^{p-1} \equiv 1 \pmod{p}$ for any a not a multiple of p.*

Proof. As a is coprime to n, we have $[a] \in U_n$. As "exponent divides group order" (Corollary 26), we have $[a]^{|U_n|} = [1]$, which means $a^{\varphi(n)} \equiv 1 \pmod{n}$. We have seen that for a prime p, $\varphi(p) = p - 1$. □

Comment: If you want to use this as a proof of Fermat-Euler in a "non-groups" context, you must (at least) add the proof that U_n is a group.

We can use Lagrange to help us find subgroups:

Examples: ◇ D_{10}

possible subgroup sizes	must be
1	$\{e\}$
2	elements must have order 2 → 5 such
5	must be cyclic, e plus 4 elements of order 5. So only one.
10	D_{10}

◇ D_8

possible subgroup sizes	searching gives
1	$\{e\}$
2	5 such (4 reflections, one rotation 180°)
4	3 such (one of which is cyclic)
8	D_8

Exercise: Use Lagrange to help you find all subgroups of the cyclic group C_n.

Remark: The converse of Lagrange is false! That is, if $k \mid |G|$, there is not necessarily a subgroup of order k. E.g. $|A_4| = 12$, and A_4 has no subgroup of order 6 (see Sheet 2 Q4). (C.f. Cauchy Theorem (Thm 53): this is different for primes.)

We can also use Lagrange to determine what small groups must look like.

32 Proposition: ("groups of order 4")
A group of order 4 is isomorphic to either C_4 or $C_2 \times C_2$.

Proof. Let $|G| = 4$. By Lagrange, possible element orders are: 1 (only e), 2, 4. If there is an element $a \in G$ of order 4, then $G = \langle a \rangle \cong C_4$.

If not, then all non-identity elements have order 2. So by Sheet 1 Q8, G is abelian. Take two elements of order 2, say $b, c \in G$. Then $\langle b \rangle = \{e, b\}$, $\langle c \rangle = \{e, c\}$, so $\langle b \rangle \cap \langle c \rangle = \{e\}$. As G is abelian, $\langle b \rangle$ and $\langle c \rangle$ commute. The element $bc = cb$ also has order 2 and is the only element of G left, so $G = \langle b \rangle \cdot \langle c \rangle$, so by the "Direct Product Theorem" (Proposition 13), $G \cong \langle b \rangle \times \langle c \rangle \cong C_2 \times C_2$. □

To determine groups of size 6 we also use Lagrange, but we need normal subgroups, so we will only do it in the next chapter.

Left or right cosets

We could have proved Lagrange with right cosets.

As $|aH| = |H|$ and similarly $|H| = |Ha|$, left and right cosets have the same size. Are they the same?

Example: a) $G = (\mathbb{Z}, +)$, $H = 2\mathbb{Z}$. We have

$$0 + 2\mathbb{Z} = \{ \text{ all even numbers } \} = 2\mathbb{Z} + 0$$
$$1 + 2\mathbb{Z} = \{ \text{ all odd numbers } \} = 2\mathbb{Z} + 1$$

so left cosets equal right cosets.

Of course, if G is abelian, we have $aH = Ha$ for all $a \in G$, and any subgroup $H \leqslant G$.

b) $G = D_6 = \langle r, s \mid r^3 = e = s^2, rs = sr^{-1} \rangle \cong S_3$. $|G| = 6$. Let $K = \langle r \rangle \cong \langle (123) \rangle$, an order 3 subgroup.

The cosets partition G, so they must be

$$K = \{e, r, r^2\} \cong \{e, (123), (132)\}$$
$$\text{and} \quad sK = \{s, sr = r^2 s, sr^2 = rs\} = Ks$$
$$(\text{or} \quad (12)K = \{(12), (23), (13)\} = K(12))$$

So for all $a \in G$, $aK = Ka$.

c) Take $G = D_6 \cong S_3$ again, but $H = \langle s \rangle \cong \langle (12) \rangle$, order 2.

left cosets	right cosets
$H = \{e, s\} \cong \{e, (12)\}$	$H = \{e, s\} \cong \{e, (12)\}$
$rH = \{r, rs = sr^{-1}\}$	$Hr = \{r, sr = r^2 s\}$
$\cong \{(123), (13)\} = (123)H$	$\cong \{(123), (23)\} = H(123)$
$r^2 H = \{r^2, r^2 s = sr\}$	$Hr^2 = \{r^2, sr^2 = rs\}$
$\cong \{(132), (23)\} = (132)H$	$\cong \{(132), (13)\} = H(132)$

They don't coincide.

K and H are "different kinds of subgroups", see next chapter.

CHAPTER 4

Quotient groups

Normal subgroups

Definition: A subgroup K of G is a **normal** subgroup if for all $a \in G$ and for all $k \in K$ we have $aka^{-1} \in K$. Write $K \trianglelefteq G$.

Exercise: This is equivalent to

- $\diamond$ $\forall a \in G$, we have $aK = Ka$ (left coset=right coset)
- $\diamond$ $\forall a \in G$, we have $aKa^{-1} = K$ (see later: conjugacy classes in Chapter 5, in particular Lemma 51)

From the earlier example, $H \leqslant D_6$ is not normal, but $K \trianglelefteq D_6$ is.
Every non-trivial group has at least two normal subgroups: which ones?

33 Lemma: *(i) Any subgroup of index 2 is normal.*
(ii) Any subgroup of an abelian group is normal.

PROOF. (i) If $K \leqslant G$ of index 2, then the only two possible cosets are K and $G\backslash K$ (because cosets partition G, proved in Lagrange, Thm 23). since $eK = Ke$, the other left as well as the other right coset must both be $G\backslash K$. So left and right cosets are the same.
(ii) In an abelian group we have (the stronger condition) $aka^{-1} = k$ for all $a \in G, k \in K$.
□

34 Proposition: *Every kernel is a normal subgroup.*

PROOF. Let $f\colon G \longrightarrow H$ be a group homomorphism with $\operatorname{Ker} f = K$. As seen in "Images and Kernels", for $k \in K, a \in G$, we have $f(aka^{-1}) = f(a)f(k)f(a)^{-1} = f(a)f(a)^{-1} = e$. So $aka^{-1} \in K$, so $K \trianglelefteq G$. □

So we now know that $A_n \trianglelefteq S_n$ because it is a kernel!
In fact, will see in the next sections that the kernels are *exactly* the normal subgroups.

Example: In $G = D_8$, the subgroup $K = \langle r^2 \rangle$ is normal.
Proof: Any element of G is either sr^l or r^l (for some l). Check both types: e.g. $sr^l r^2 (sr^l)^{-1} = sr^l r^2 r^{-l} s = ssr^{-2} = r^2 \in K$. The second case is an exercise.

Here is an example of how normality can be used.

35 Proposition: ("groups of order 6")
Every group of order 6 is either cyclic or dihedral.

PROOF. Let $|G| = 6$. By Lagrange, possible element orders are $1, 2, 3$ and 6. If there is $a \in G$ of order 6, then $G \cong C_6$.

If there is no element of order 6, we can only have orders $2, 3$ (other than e). By Sheet 1 Q8, there must be an element $r \in G$ of order 3 (as 6 is not a power of 2). So $\langle r \rangle \trianglelefteq G$ as it has index 2. There must also be an element $s \in G$ of order 2, by Sheet 1 Q9 (as 6 is even).

What is srs^{-1}? As $\langle r \rangle$ is normal, $srs^{-1} \in \langle r \rangle$, so

- $srs^{-1} = e$ not possible (as $r \neq e$), or
- $srs^{-1} = r$ $\Rightarrow sr = rs$ and sr has order 6 $\Rightarrow G \cong C_6$ or
- $srs^{-1} = r^2 = r^{-1}$ $\Rightarrow G$ is dihedral, i.e. $G = \langle r, s \mid r^3 = e = s^2, srs^{-1} = r^{-1} \rangle \cong D_6$.

□

Quotients

We will now investigate when we can form a group out of cosets.

This is a part that many students find difficult to get their head round first time, because sets (the cosets) suddenly become elements of some other set. So to get a bit of a feeling for it, I will describe a little demonstration that can help. Take the numbers 0 to 11 with addition mod 12, and randomly pair them up to make equivalence classes (of some not-further-determined equivalence relation). Say we have paired up $\{1, 4\}$, $\{3, 8\}$, $\{7, 2\}$, ... If we now want to add them, we could try saying $\{1, 4\} + \{7, 2\} = \{3, 8\}$ because $1 + 7 = 8$, but we could equally well have used 4 and 7, then we'd need to get the pair of numbers containing 11. So this is not well-defined. We are trying to define the addition of two sets by adding some representatives inside the sets, but we get different answers for different choices.

Instead, now pair up the numbers in the cosets of the subgroup $\{0, 6\}$ of $\mathbb{Z}_{12}$. So now we have $\{0, 6\}$, $\{1, 7\}$, $\{2, 8\}$, $\{3, 9\}$ and so on up to $\{5, 11\}$. Now if you try adding two of these sets, regardless of which representatives you choose to add you will get the same coset as your answer! For example $\{1, 7\} + \{3, 9\} = \{4, 10\}$, because $1 + 3 = 4$ or because $1 + 9 = 10$ or because $7 + 3 = 10$ or because $7 + 9 = 16 = 4 \pmod{12}$. So any of the choices we make give the same answer. Try it also with the cosets of the subgroup $\{0, 3, 6, 9\}$. Let's do it properly mathematically now.

36 Proposition: *Let $K \trianglelefteq G$. The set $(G : K)$ of (left) cosets of K in G is a group under the operation $aK * bK = abK$.*

Proof. We will show that the operation is in fact well-defined, and satisfies the group axioms.

Well-defined: If $aK = a'K$ and $bK = b'K$, then $a' = ak_1$ and $b' = bk_2$ for some $k_1, k_2 \in K$. So $a'b' = ak_1bk_2 = abk_3k_2 \in abK$ for some $k_3 \in K$, as $Kb = bK$.

Closure: If aK, bK are cosets, then so is abK.

Identity: $eK = K$ is the identity (clear from the definition of the group operation).

Inverses: $a^{-1}K$ is the inverse to aK (clear from def. of the operation *once it's well-defined*).

Associativity: follows from associativity in G. □

Alternative way of using the normality in the proof of well-definedness: We start with $a'b' = ak_1bk_2$. We want to get to $a'b' = abk$ for some $k \in K$. So let's try to make it like that: $a'b' = ak_1bk_2 = ab\ b^{-1}k_1b\ k_2$. Here we added the b after the a because we wanted it there, but to keep the equation the same, we have to also include b^{-1}. But now $b^{-1}k_1b \in K$ because K is normal, so we get $a'b' = abk_3k_2$ as we did in the proof above.

Definition: This group is called the **quotient group** (or factor group) of G by K, and written G/K.

Examples: a) Let $G = \mathbb{Z}$ and $K = n\mathbb{Z}$ (which is normal as G is abelian). The cosets are $n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$. G/K gives "addition mod n". We write

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

In fact these are the only quotient groups of $\mathbb{Z}$, see "subgroups of $\mathbb{Z}$" (Proposition 5).

b) Recall the example $K \trianglelefteq D_6$ from Section Left and right cosets.

We have $D_6 = \langle r, s \mid r^3 = e = s^2, sr = r^{-1}s \rangle$ and $K = \langle r \rangle \trianglelefteq D_6$ (as it has index 2). There are two cosets K and sK, so D_6/K has order 2, so $D_6/K \cong C_2$.

c) Now we use $K = \langle r^2 \rangle \trianglelefteq D_8 = \langle r, s \mid r^4 = e = s^2, sr = r^{-1}s \rangle$ (from Section Normal subgroups). G/K should have $|D_8| : |K| = 4$ elements. [Or you might be more used to

the notation $|D_8|/|K| = 4$.]

$$G/K = \{K, rK = r^3K, sK = sr^2K, srK = sr^3K = rsK\}$$
$$\cong \{e, x, y, xy\} \cong C_2 \times C_2$$

by Propsition 32 "groups of order 4", as all elements have order 2.

Remarks: ◇ If G is abelian, then G/K is also abelian.
◇ The *set* $(G : H)$ of left cosets also exists for non-normal subgroups $H \leqslant G$, but the group operation given above is *not well-defined*!!

Non-Example: Try D_6 with $H = \langle s \rangle$. We saw the cosets in Section Left and right cosets. E.g. $rH * r^2H = r^3H = H$, but $rH = rsH$ and $r^2H = srH$, and $rssrH = r^2H \neq H$.

37 Lemma: *Given $K \trianglelefteq G$, the map $q\colon G \longrightarrow G/K$ sending a to aK is a surjective group homomorphism (called the **quotient map**).*

Proof. $q(ab) = abK = aK * bK = q(a) * q(b)$ by definition. It is clearly surjective. □

Example: d) Let $G = C_n$ and $H \leqslant C_n$ (we've seen that H is also cyclic).
Say $C_n = \langle c \mid c^n = e \rangle$ and $H = \langle c^k \rangle \cong C_l$ where $kl = n$.

$$q\colon C_n \longrightarrow C_n/H$$
$$c^m \longmapsto c^m H$$

$\operatorname{Ker} q = \{c^m \mid c^m H = H\} = H$.
What does the quotient group look like?

$$C_n/H = \{H, cH, c^2H, \ldots, c^{k-1}H\} = \langle cH \rangle \cong C_k.$$

Slogan: "Subgroups and quotients of cyclic groups are cyclic."

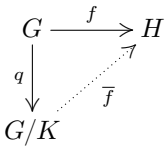
Remark: Quotient groups are *not* subgroups of G! They contain different kinds of elements (they are not even subset). They may not even be *isomorphic* to any subgroups.
e.g. $\mathbb{Z}$: quotient groups are $\mathbb{Z}/n\mathbb{Z}$ (all finite)
subgroups are $m\mathbb{Z}$ (all infinite)
(In some sense "quotients are the opposite of (normal) subgroups" cf Part III Category Theory.)

The Isomorphism Theorem

We saw that all kernels are normal subgroups.
Given $K \trianglelefteq G$, we have the quotient map $q\colon G \longrightarrow G/K$ with $\operatorname{Ker} q = K$. So "normal subgroups are exactly the kernels of group homomorphisms".
Now we refine this even more:

38 Theorem: (Isomorphism Theorem)
Let $f\colon G \longrightarrow H$ be a group homomorphism with $\operatorname{Ker} f = K$. Then $K \trianglelefteq G$ and $G/K \cong \operatorname{Im} f$.

Proof. We have proved $K \trianglelefteq G$ already (Proposition 34).



Define $\overline{f}\colon G/K \longrightarrow H$ by $\overline{f}(aK) = f(a)$ (so that we get $\overline{f}q = f$). We check that this is well-defined: if $a_1K = a_2K$, then $a_2^{-1}a_1 \in K$ by "same coset check" (Fact 24), so $e = f(a_2^{-1}a_1) = f(a_2)^{-1}f(a_1)$, so $f(a_2) = f(a_1)$, and $\overline{f}(a_1K) = \overline{f}(a_2K)$ as required.

$\overline{f}$ is a homomorphism: $\overline{f}(aK * bK) = \overline{f}(abK) = f(ab) = f(a)f(b) = \overline{f}(aK)\overline{f}(bK)$.

$\overline{f}$ is injective: If $\overline{f}(aK) = \overline{f}(bK)$ (i.e. $f(a) = f(b)$), then $f(b^{-1}a) = f(b)^{-1}f(a) = e$, so $b^{-1}a \in K$, so $aK = bK$ by "same coset check".

$\overline{f}$ is clearly surjective onto $\mathrm{Im}f$.

So $\overline{f}$ gives an isomorphism $G/K \cong \mathrm{Im}f$ $(\leqslant H)$. □

Remarks: ◇ If $f\colon G \longrightarrow H$ is injective, then $\mathrm{Ker}\, f = \{e\}$, so $G/K \cong G$ and G is isomorphic to a subgroup of H (write $G \lesssim H$; e.g. inclusion).

◇ If $f\colon G \longrightarrow H$ is surjective, then $\mathrm{Im}f = H$, so then $G/K \cong H$.

Slogan: "Homomorphic images are quotients."

Examples: a) Consider the determinant homomorphism $\det\colon \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$. The kernel is $\mathrm{Ker}(\det) = \mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A = 1\}$ and the image is $\mathrm{Im}f = \mathbb{R}^*$, since for $x \in \mathbb{R}^*$, we have $\begin{vmatrix} x & & & \\ & 1 & 0 & \\ & & \ddots & \\ & 0 & & 1 \end{vmatrix} = x$.

So by the Isomorphism Theorem $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$.

b) Define $\theta\colon (\mathbb{R}, +) \longrightarrow (\mathbb{C}^*, \cdot)$ by $\theta(r) = e^{2\pi ir}$.

It is a group homomorphism: $\theta(r+s) = e^{2\pi i(r+s)} = e^{2\pi ir}e^{2\pi is} = \theta(r)\theta(s)$. Its kernel is $\mathbb{Z} \trianglelefteq \mathbb{R}$.

What is the image? We use the Isomorphism Theorem to get $\mathbb{R}/\mathbb{Z} \cong \mathrm{Im}\theta =: (S_1, \cdot)$, which we can take as a definition of the **unit circle**.

c) Let $G = \mathbb{Z}_p^* = \mathbb{Z}/p\mathbb{Z}\backslash\{0\}$, for p prime $(p \neq 2)$.

The map $f\colon G \longrightarrow G$ defined by $f(a) = a^2$ is a group homomorphism: $(ab)^2 = a^2b^2$ as $(\mathbb{Z}/p\mathbb{Z})^*$ is abelian. The kernel is $\mathrm{Ker}\, f = \{\pm 1\} = \{1, p-1\}$. So we see that $\mathrm{Im}f \cong G/\mathrm{Ker}\, f$ must have order $\frac{p-1}{2}$ (these are the "quadratic residues").

39 Lemma: ("essential uniqueness of cyclic groups")
Any cyclic group is isomorphic to either $(\mathbb{Z}, +)$ *or* $(\mathbb{Z}/n\mathbb{Z}, +_n)$ *for some* $n \in \mathbb{N}$.

Proof. Let $G = \langle c \rangle$ be cyclic. Define

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow G \\ m &\longmapsto c^m \end{aligned}$$

f is a group homomorphism: $c^{m_1+m_2} = c^{m_1}c^{m_2}$.

f is clearly surjective. $\mathrm{Ker}\, f \trianglelefteq \mathbb{Z}$, so either

◇ $\mathrm{Ker}\, f = \{e\}$, so f is an isomorphism, so $G \cong \mathbb{Z}$.

◇ $\mathrm{Ker}\, f = \mathbb{Z}$, then $G \cong \mathbb{Z}/\mathbb{Z} = \{e\} = C_1$.

◇ $\mathrm{Ker}\, f = n\mathbb{Z}$ for some $n \in \mathbb{N}$ (these are the only subgroups of $\mathbb{Z}$, see Prop. 5). Then $G \cong \mathbb{Z}/n\mathbb{Z} \cong C_n$ by the Isomorphism Theorem.

□

Definition: A group G is **simple** if it has no non-trivial proper normal subgroups. (i.e. only $\{e\}$ and G).

Example: ◇ C_p with p prime is simple (but boring).

◇ A_5 is simple (proof later, Theorem 59).

The finite simple groups are the building blocks of all finite groups. All finite simple groups have been classified.

Note that for $K \trianglelefteq G$ with $\{e\} \neq K \neq G$, we have $|K| < |G|$ and $|G/K| < |G|$.

CHAPTER 5

Group actions

Groups acting on sets

Recall the symmetries of an n-gons or Sym$X$: the group elements "do something" to the set of vertices or the set X.

Definition: Let X be a set, G a group. An **action** of G on X is a function $\theta\colon G \times X \longrightarrow X$ satisfying

0. $\theta(g,x) \in X$ for all $g \in G, x \in X$;
1. $\theta(e,x) = x$ for all $x \in X$;
2. $\theta(g,\theta(h,x)) = \theta(gh,x)$ for all $g,h \in G, x \in X$.

Alternative notations:

$$\begin{array}{c|c} \theta(g,x) = g\cdot x = g(x) \in X & \theta(g,-) = \theta_g\colon X \longrightarrow X \\ \theta(e,x) = e\cdot x = e(x) = x & \theta_e(x) = x \text{ or } \theta_e = 1_X \\ \theta(g,\theta(h,x)) = \theta(gh,x) \text{ or } g(hx) = (gh)x \text{ or } g(h(x)) = (gh)(x) & \theta_g{\circ}\theta_h = \theta_{gh} \end{array}$$

Examples: a) Trivial action: take any group G and any set X, with $\theta(g,x) = x$ for all g,x. "G does nothing".

b) S_n acts on $\{1,\dots,n\}$ by permutation.

c) D_{2n} acts on (the vertices of) a regular n-gon and/or acts on $\{1,\dots,n\}$.

d) Rotations of a cube act on: faces of the cube, or diagonals, or axes (= pairs of opposite faces), or...

Remark: Compare b), c): different groups can act on the same set. d): One group can act on different sets.

40 Lemma: *For each $g \in G$, $\theta(g,-) = \theta_g\colon X \longrightarrow X$ is a bijection.*

Proof. As $\theta(g,\theta(g^{-1},x)) = \theta(gg^{-1},x) = \theta(e,x) = x$ for all $x \in X$, we have $\theta_g{\circ}\theta_{g^{-1}} = 1_X$, the identity on X. Similarly $\theta_{g^{-1}}{\circ}\theta_g = 1_X$, so θ_g is a bijection (with inverse $\theta_{g^{-1}}$). □

41 Proposition: ("Alternative Action Definition")
Let G be a group, X a set. Then $\theta\colon G \times X \longrightarrow X$ with $\theta(g,x) = \theta_g(x)$ is an action if and only if $\varphi\colon G \longrightarrow$ Sym$X$ with $\varphi(g) = \theta_g$ is a group homomorphism.

Proof. "⇒" By Lemma 40, $\theta_g\colon X \longrightarrow X$ is a bijection, so indeed $\theta_g \in$ Sym$X$. We have $\varphi(gh) = \theta_{gh} = \theta_g{\circ}\theta_h = \varphi(g){\circ}\varphi(h)$, so φ is a group homomorphism.

"⇐" Given $\varphi\colon G \longrightarrow$ Sym$X$ a group homomorphism, and defining $\theta\colon G \times X \longrightarrow X$ by $\theta(g,x) = \varphi(g)(x)$, the resulting θ is an action:

0. As $\varphi(g) = \theta_g \in$ Sym$X$, $\theta(g,x) = \theta_g(x) \in X$.
1. $\varphi(e) = 1_X = \theta_e$, so $\theta_e(x) = x$ for all x.
2. $\varphi(gh) = \varphi(g){\circ}\varphi(h)$, so $\theta_g{\circ}\theta_h = \theta_{gh}$.

□

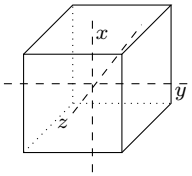
Definition: Given an action of G on X, the **kernel** of the action is $\mathrm{Ker}(\varphi\colon G \longrightarrow \mathrm{Sym}X)$.

Note: These are all the elements that "act as the identity". We have just shown that they form a (normal) subgroup of G.

$$\mathrm{Ker}\,\varphi = K \trianglelefteq G \qquad \text{and} \qquad G/K \lesssim \mathrm{Sym}X.$$

Examples: a) D_{2n} acting on n vertices $\{1,\dots,n\}$ gives $\varphi\colon D_{2n} \longrightarrow S_n$ with $\mathrm{Ker}\,\varphi = \{e\}$. (This formalises our view of D_{2n} as a subgroup of S_n.)

b) Let G be the rotations of a cube, and let it act on the axes (=pairs of opposite faces) x, y, z.



This gives $\varphi\colon G \longrightarrow S_3$. Then rotation around any of these axes by 180° acts as the identity on $\{x, y, z\}$. So here the kernel of the action has (at least) 4 elements: e, and those three 180° rotations. (In fact we will see later: these 4 are exactly the kernel, there are no more; c.f. Section Using actions.)

Definition: An action is called **faithful** if $\mathrm{Ker}\,\varphi = \{e\}$.

Orbits and Stabilisers

Which elements can we "reach" from some $x \in X$? Which group elements fix x?

Definition: Given an action of G on X and $x \in X$, the **orbit** of x is

$$\mathrm{orb}(x) = G(x) = \{y \in X \mid \exists g \in G \text{ s.t. } g(x) = y\} \subseteq X$$

and the **Stabiliser** of x is

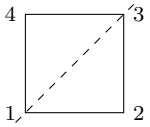
$$\mathrm{Stab}(x) = G_x = \{g \in G \mid g(x) = x\} \subseteq G$$

The orbit of x is the set of elements we can reach from x, and the stabiliser of x is the set of group elements which fix x.

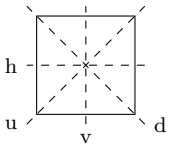
42 Lemma: $\mathrm{Stab}(x)$ *is a subgroup of* G.

Proof. ◇ $e(x) = x$ so $\mathrm{Stab}(x)$ is non-empty.
◇ If $g, h \in \mathrm{Stab}(x)$, then $gh^{-1}(x) = g(x) = x$ so $gh^{-1} \in \mathrm{Stab}(x)$.
So $\mathrm{Stab}(x)$ is a subgroup by the super-efficient subgroup criterion (Lemma 4). □

Examples: a) Let D_8 act on the corners of a square, so $X = \{1, 2, 3, 4\}$. Then $\mathrm{orb}(1) = X$ and $\mathrm{Stab}(1) = \{e,$ reflection in diagonal through corner $1\}$.



b) Let D_8 act on the symmetry lines of a square, say called v, h, u, d as in the picture below. Here $\mathrm{orb}(h) = \{h, v\}$, $\mathrm{orb}(u) = \{u, d\}$.



c) Let $\langle(12)\rangle$ act on $\{1,2,3\}$.

$$\text{orb}(1) = \{1,2\} \quad \text{and} \quad \text{orb}(3) = \{3\}$$
$$\text{Stab}(1) = \{e\} \quad \text{and} \quad \text{Stab}(3) = \{e,(12)\}$$

d) Let the rotations of a cube act on the three axes (=pair of opposite faces) x, y, z (as before). We can convince ourselves that $\text{orb}(x) = \{x, y, z\}$. The stabiliser is harder. We can find $\text{Stab}(x) \supseteq \{e,$ any rotation in axis x (3 such), 180° rotation in axis y or axis $z\}$.

But it is hard to know if we have found all elements of the stabiliser. See later to learn how to do that (using the Orbit-Stabiliser Theorem (Theorem 44), this is worked out in Chapter 5, Section Applications).

Exercise: There are two more elements in the stabiliser above. Can you find them using the Taylor-Cube? You can find a net for the "Taylor-Cube" on the Moodle course page, my blog or on Gareth Taylor's website.

Definition: An action of G on X is called **transitive** if $\text{orb}(x) = X$ for all $x \in X$.
"You can reach any element from any element."

43 Lemma: *The orbits of an action partition X.*

Proof. Let G act on X.
(i) $\forall x \in X$, $x \in \text{orb}(x)$ as $e(x) = x$.
(ii) If $z \in \text{orb}(x) \cap \text{orb}(y)$, then $\exists g_1 \in G$ s.t. $g_1(x) = z$ and $\exists g_2 \in G$ s.t. $g_2(y) = z$. So $x = g_1^{-1}(g_2(y))$. Then for any $w \in \text{orb}(x)$ with $g(x) = w$, we have $g(g_1^{-1}(g_2(y))) = w$ so $w \in \text{orb}(y)$. So $\text{orb}(x) \subseteq \text{orb}(y)$, and similarly $\text{orb}(y) \subseteq \text{orb}(x)$, so orbits are disjoint or equal.

Therefore the orbits partition X. □

Remember the proof that disjoint cycle notation works (Theorem 16): we were really finding the orbits, which are disjoint and that is why it all worked.

44 Theorem: (Orbit-Stabiliser)
Let the finite group G act on the set X. Then for any $x \in X$, we have

$$|G| = |\text{orb}(x)||\text{Stab}(x)|.$$

Proof. "turn it into Lagrange" (Beardon calls it "geometric version of Lagrange")
Idea: We show that each point in the orbit of x corresponds to a particular coset of $\text{Stab}(x)$.
$\text{Stab}(x)$ is a subgroup of G (by Lemma 42). Then for $y \in \text{orb}(x)$, say with $g(x) = y$, the set of all h which take x to y is the left coset of $\text{Stab}(x)$ determined by g:

$$\{h \in G \mid y = h(x)\} = g\text{Stab}(x)$$

because $h(x) = y = g(x) \Leftrightarrow g^{-1}h(x) = x \Leftrightarrow g^{-1}h \in \text{Stab}(x) \Leftrightarrow h \in g\text{Stab}(x)$. (In the last step we used the "same coset check", Fact 24.) Each coset has size $|\text{Stab}(x)|$, and there are $|\text{orb}(x)|$ many points in the orbit which all give different cosets (i.e. each coset corresponds to a point in the orbit), so

$$|G| = |\text{orb}(x)||\text{Stab}(x)|.$$

□

Examples: a) In Chapter 1, Section Symmetries of a square we worked out "how big is D_{2n}". Now we can do it using Orbit-Stabiliser: D_{2n} acts on $\{1,\dots,n\}$ transitively, so $|\text{orb}(1)| = n$. $\text{Stab}(1) = \{e,$ reflection in line through $1\}$, so $|D_{2n}| = n \cdot 2$. The reflection in the line through 1 represents the part of the argument where we said "once 1 is fixed, 2 can go in two different places".

Note: if the action is transitive, then all stabilisers have same size.

b) Let $\langle(12)\rangle$ act on $\{1,2,3\}$ as before. We saw

$$\begin{aligned} \text{orb}(1) &= \{1,2\} && \text{and} && \text{orb}(3) &= \{3\} \\ \text{Stab}(1) &= \{e\} && \text{and} && \text{Stab}(3) &= \{e,(12)\} \end{aligned}$$

so the sizes are different, but in each case multiply to 2.

Exercise: see what you get with e.g. $\langle(123)(45)(6789)\rangle$ acting on $\{1,\dots,9\}$.

c) Let S_4 act on $X = \{1,2,3,4\}$. We have $\text{orb}(1) = X$ and $|S_4| = 24$, so we know that $|\text{Stab}(1)| = |S_4|/|\text{orb}(1)| = 24/4 = 6$. That makes it easier to find: clearly $S_{\{2,3,4\}} \cong S_3$ fixes 1, so $S_{\{2,3,4\}} \subseteq \text{Stab}(1)$, but by sizes this gives $S_{\{2,3,4\}} = \text{Stab}(1)$.

Standard actions

We will now learn about some actions which come up again and again, and some of their consequences.

45 Lemma: (left regular action)
Every group G acts on itself by left multiplication. This action is faithful and transitive.

PROOF. We check the three conditions for an action:

0. $\forall g \in G, x \in G$, $gx \in G$.
1. $e \cdot x = x$ for all $x \in G$ — by identity axiom.
2. $g(hx) = (gh)x$ — by associativity.

So this is indeed an action.

The action is faithful: if $gx = x$ for all $x \in X$, then $g = e$ by uniqueness of identity (Prop. 1).

The action is transitive: given $x, y \in G$, then $yx^{-1} = g \in G$ and $gx = yx^{-1}x = y$. □

This action gives rise to the important theorem:

46 Theorem: (Cayley)
Every group is isomorphic to a subgroup of some symmetric group.

PROOF. Take the left regular action of G on itself. This gives a group homomorphism $\varphi\colon G \longrightarrow \text{Sym}G$, with kernel $\text{Ker}\,\varphi = \{e\}$ as the action is faithful. So by the Isomorphism Theorem (Theorem 38), $G \cong \text{Im}\varphi \leqslant \text{Sym}G$. □

47 Lemma: (left coset action)
Let $H \leqslant G$. Then G acts on the left cosets of H by left multiplication, transitively.

PROOF. We check the three conditions for an action:

0. $g(aH) = gaH$ is a coset of H.
1. $e(aH) = aH$ for all cosets aH.
2. $g_1(g_2(aH)) = g_1((g_2a_2)H) = (g_1g_2)aH$ by associativity in G.

So this is indeed an action. Given aH, bH, we have $ba^{-1} \in G$ and $ba^{-1}(aH) = bH$, so the action is transitive. □

Note: if $H = \{e\}$, this is just the left regular action.

Definition: Given $a, b \in G$, the element $bab^{-1} \in G$ is the **conjugate** of a by b.

48 Lemma: (conjugation action)
Any group G acts on itself by conjugation.

PROOF. We check the three conditions for an action:
0. $g(x) = gxg^{-1} \in G$ for $g, x \in G$.
1. $e(x) = exe^{-1} = x$ for all $x \in G$.
2. $g(h(x)) = g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1}$

So this is indeed an action. □

This action is so important that the kernel, orbits and stabilisers of it have special names.

Definition: The kernel of this action is the **centre** of G:

$$Z(G) = \{g \in G \mid gag^{-1} = a \quad \forall a \in G\} = \{g \in G \mid ga = ag \quad \forall a \in G\}$$

"elements that commute with everything".

(This is also sometimes written $C(G)$ but that can be confusing with centraliser notation coming next.)

The orbits of this action are called **conjugacy classes**

$$\mathrm{ccl}(a) = \{b \in G \mid \exists g \in G \text{ s.t. } gag^{-1} = b\}.$$

The stabilisers of this action are called **centralisers**

$$C_G(a) = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid ga = ag\}$$

"elements that commute with a."

Remark: $Z(G) = \bigcap_{g \in G} C_G(g)$ (Exercise)

Slogan: "Conjugate elements have many of the same properties."

Exercise: Conjugate elements have the same order, same size centralisers, ... cf ccls in S_n.

Conjugacy is used a lot in all sorts of different areas of maths, like geometry, algebra, also physics, to make situations easier to handle. For example, when considering a rotation in $\mathbb{C}$ about any point, we can first translate that point to 0, then do the rotation around 0, which is very easy, and then translate 0 back to the original point. In similar ways conjugacy is used to consider an "easier" but entirely equivalent situation. We will use it a lot when we work with Möbius maps in the last chapter.

Conjugacy and normal subgroups are very closely related. First we see:

49 Lemma: ("conjugation action restricts to normal subgroups")
Let $K \trianglelefteq G$. Then G acts by conjugation on K.

PROOF. For all $g \in G, k \in K$, we have $gkg^{-1} \in K$, so the map $G \times K \longrightarrow K$ sending (g, k) to gkg^{-1} does land in K. We still have $eke^{-1} = k$ for all $k \in K$, and still have $(gh)k(gh)^{-1} = g(hkh^{-1})g^{-1}$. □

And now we look the other way, using conjugacy to determine which subgroups are normal.

50 Proposition: ("Normal = $\bigcup$ccls")
Normal subgroups are exactly those subgroups which are unions of conjugacy classes.

PROOF. Let $K \trianglelefteq G$. Then if $k \in K$, so is gkg^{-1} for all $g \in G$, so $\mathrm{ccl}(k) \subseteq K$. Conversely, if K is a union of ccls and a subgroup of G, then for all $k \in K, g \in G$, we have $gkg^{-1} \in K$, so K is normal. □

51 Lemma: (conjugation action on subgroups)
Let X be the set of subgroups of G. Then G acts by conjugation on X.

PROOF. We check the three conditions of an action:

0. If $H \leqslant G$, then we have to show that gHg^{-1} is also a subgroup:
   - $e \in H \Rightarrow geg^{-1} = e \in gHg^{-1}$ so it is non-empty.
   - Any two elements in gHg^{-1} are of the form gag^{-1}, gbg^{-1} for some $a, b \in H$. Then $gag^{-1}(gbg^{-1})^{-1} = gag^{-1}gb^{-1}g^{-1} = gab^{-1}g^{-1} \in gHg^{-1}$ as $ab^{-1} \in H$.

   So by the super-efficient subgroup criterion (Lemma 4), $gHg^{-1} \leqslant G$.
1. $eHe^{-1} = H$.
2. $g_1(g_2Hg_2^{-1})g_1^{-1} = (g_1g_2)H(g_1g_2)^{-1}$.

So this is indeed an action. □

Remark: If $K \trianglelefteq G$, then the ccl of K under this action is just $\{K\}$. "Normal subgroups are exactly the ones with singleton ccls."

Exercise: If H_1, H_2 are conjugate subgroups, then they are isomorphic. In particular, they have the same size.

Definition: The stabilisers of this action are called **normalisers**

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

"$N_G(H)$ is the largest subgroups of G such that $H \trianglelefteq N_G(H)$." (Exercise)
Clearly $H \leqslant N_G(H)$.

There is a connection between actions in general and conjugation of subgroups:

52 Lemma: ("Stabilisers of elements in same orbit are conjugate")
Let G act on X, and let $g \in G, x \in X$. Then

$$\mathrm{Stab}(g(x)) = g\mathrm{Stab}(x)g^{-1}$$
$$(or \quad G_{g(x)} = gG_xg^{-1} \quad)$$

PROOF. Example Sheet 3. □

So they are in particular isomorphic.

Using actions

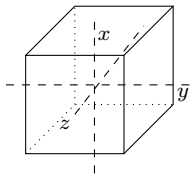
Using actions, we can find out lots of things about groups. We will give some examples here.
We can use the Orbit-Stabiliser Theorem to find sizes of groups.

Example: (Cube) Let G^+ be the group of all rotations of a cube, acting on the vertices. So $X = \{\text{vertices}\}, |X| = 8$. The action is transitive (convince yourself).

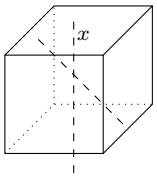
What is the stabiliser of vertex 1? It is exactly all rotations in the axis through 1 and the diagonally opposite vertex. There are three of those (including e). So $|G| = |\mathrm{orb}(1)||\mathrm{Stab}(1)| = 8 \cdot 3 = 24$.

Having found the size of a group, we can also use the Orbit-Stabiliser Theorem to find sizes of stabilisers.

Example: (Cube) Let G^+ be rotations of a cube as above, but now acting on the three axes (=pairs of opposite faces), let us call them x, y, z.



We see that this action is transitive, so $|\text{orb}(x)| = 3$. So $|\text{Stab}(x)| = 24/3 = 8$. This helps to find the elements of the stabiliser: we certainly have any rotation in the axis x, which gives 4 elements (this includes e). Then we have rotations of 180° in the axis y and in the axis z. We know we are missing two so we look a bit harder and find that rotation by 180° in the axis which goes through the midpoints of edges parallel to the axis x also fixes x. There are two of these, so now we know all elements in the stabiliser. If we hadn't known the size, we may not have thought of looking for these last two.



Notice that the first four elements we mentioned keep the endpoints of the axis x (i.e. both faces of the "pair of opposite faces") fixed, whereas the other four switch them.

Looking at the homomorphism $\varphi\colon G^+ \longrightarrow S_3$ induced by this action, we now see that the kernel of φ is the intersection of the stabilisers of x, y and z, so contains exactly four elements: e and rotation by 180° around any of the three axes.

All this is very nicely visualised on the "Taylor-Cube", which you can find on the Moodle course page, my blog or on Gareth Taylor's website.

We have used the alternative action definition (Prop. 41) via a homomorphism to S_n above. We can use this homomorphism also to say something about the existence of normal subgroups or existence of particular size subgroups.

Example: G finite, $H \leqslant G$ of index n, G acts on left cosets of H by left multiplication. This gives a group homomorphism (which is non-trivial for $H \neq G$)

$$\varphi\colon G \longrightarrow S_n \qquad (\text{as } n \text{ cosets of } H)$$

Now $\text{Ker}\,\varphi \trianglelefteq G$, and we know $\text{Ker}\,\varphi \neq G$. So
either we have found a normal subgroup if we know such an H exists (it could be $\{e\}$).
or if G is simple, we know $\text{Ker}\,\varphi = \{e\}$, so that tells us something about the possibilities of n:

$$n! \geqslant |G|.$$

I would like you to use this as a technique rather than quote it as a result, as it is such a flexible argument.

Further refinement: Consider

$$G \xrightarrow{\varphi} S_n \xrightarrow{\text{sgn}} \{\pm 1\}$$

The kernel of this composite is normal in G. If G is simple, $\text{Ker}(\text{sgn}\circ\varphi) = \{e\}$ or G. Look at sizes: can it be $\{e\}$? If it is G, we know that $\text{Im}\varphi \leqslant A_n$, so $\frac{n!}{2} \geqslant |G|$.

We've seen on Sheet 1 that if $|G|$ is even, then G has an element of order 2. In fact, we can use our knowledge of actions to prove the very useful:

53 Theorem: (Cauchy)
Let G be a finite group, p a prime dividing $|G|$. Then G has an element of order p.

Idea of proof: An element of order p satisfies $a \cdot a \cdots a = e$, where we have p copies of a. So we look at p-tuples $(a_1, a_2, \ldots, a_p)$ which multiply to e. A tuple of form $(a, a, \ldots, a)$ is special amongst these: it doesn't change under "rotation" to $(a_2, a_3, \ldots, a_p, a_1)$. So we act on such p-tuples by this "rotation", and use the fact that orbits partition the set and some knowledge about sizes to imply the existence of a size 1 orbit.

PROOF. G, p fixed. Consider $G^p = G \times \cdots \times G$ (p copies of G), the set of p-tuples of G. Let $X \subseteq G^p$ be $X = \{(a_1, \ldots, a_p) \in G^p \mid a_1 \cdots a_p = e\}$ "tuples that multiply to the identity". In particular, if an element b has order p, then $(b, b, \ldots, b) \in X$. (In fact, if $(b, b \ldots, b) \in X$ and $b \neq e$, then b has order p as p is prime.)

Now let $H = \langle h \mid h^p = e \rangle \cong C_p$ be a cyclic group of order p with generator h. Let H act on X by "rotation": $h(a_1, \ldots, a_p) = (a_2, \ldots, a_p, a_1)$. This is an action:

0. If $a_1 \cdots a_p = e$, then $a_1^{-1} = (a_2 \cdots a_p)$, so also $(a_2 \cdots a_p)a_1 = e$, so $h(a_1 \cdots a_p) \in X$.
1. $e(a_1, \ldots, a_p) = (a_1, \ldots, a_p)$
2. $h^l(a_1, \ldots a_p) = (a_{l+1}, \ldots, a_1, \ldots, a_l) = h \cdot h \cdots h(a_1, \ldots, a_p)$

As orbits partition X, the sum of all orbit sizes must be $|X|$. We know $|X| = |G|^{p-1}$ (choose first $p-1$ entries, last is inverse of their product).

Now, as $p \mid |G|$, also $p \mid |X|$. We have

$$|\mathrm{orb}(a_1, \ldots, a_p)| \cdot |\mathrm{Stab}_H(a_1, \ldots, a_p)| = |H| = p.$$

So all orbits must have size 1 or p, and they sum to $|X| = p \cdot$(something). Clearly $(e, e, \ldots, e)$ has orbit size 1. So there must be some (in fact at least $p-1$) other orbits of size 1 (to get $p \mid |X|$). These look like $\{(a, a, \ldots, a)\}$ for some $a \in G$, which has order p. □

Aside notice: given one element of order p, there must always be at least $p-2$ more as well. You can see this by considering the powers of this element, or the cyclic subgroup generated by it. It has size p, so is C_p, which is generated by any non-identity element, i.e. has $p-1$ elements of order p.

Polyhedron symmetry groups

Having found the size of the group of rotations of a cube above, we might want to know what group it is isomorphic to.

54 Proposition: $G^+ \cong S_4$.

PROOF. Let G^+ act on the four diagonal of the cube. This gives a group homomorphism $\varphi\colon G^+ \longrightarrow S_4$. We have $(1234) \in \mathrm{Im}\varphi$, by rotation around axis through top and bottom face. We also have $(12) \in \mathrm{Im}\varphi$, by rotation around axis through midpoint of edge containing 1 and 2. So by Sheet 2 Q5(d), $\mathrm{Im}\varphi = S_4$, i.e. φ is surjective. But $|G^+| = |S_4| = 24$, so φ is in fact an isomorphism.

Look at the "Taylor-Cube" to visualise all this. You can find it on the Moodle course page, my blog, or on Gareth Taylor's website. □

Now we will find out about *all* symmetries of the cube.

55 Proposition: *The group G of all symmetries of the cube is isomorphic to $S_4 \times C_2$.*

PROOF. To find the size of G, let G act on the vertices of the cube. Then as G acts transitively, $|\mathrm{orb}(1)| = 8$. The stabiliser of 1 is

$$\mathrm{Stab}(1) = \{e, 2 \text{ rotations in axis through } 1,$$
$$3 \text{ reflections in planes through 1 and an edge coming out of 1}\}$$

which has 6 elements. So $|G| = 8 \cdot 6 = 48$.

Consider the "reflection in midpoint", i.e. sending each point to its opposite on the cube. Viewing this as "$-I$" (in $\mathbb{R}^3$), we can easily see that this symmetry, call it τ, commutes with all other symmetries of the cube.

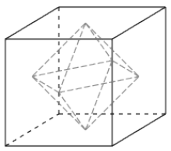
We now use a technique which is almost the same as in the Direct Product Theorem (Proposition 13) to show that $G \cong G^+ \times \langle \tau \rangle \cong S_4 \times C_2$.

From the comment above we know that τ commutes with all rotations. We also know that $G^+ \cap \langle \tau \rangle = \{e\}$. So (by the same arguments as in the Direct Product Theorem) we have an injective group homomorphism

$$\begin{aligned} G^+ \times \langle \tau \rangle &\longrightarrow G \\ (g, h) &\longmapsto gh \end{aligned}$$

which must also be surjective, since $|G| = |G^+ \times \langle \tau \rangle|$. Therefore it is an isomorphism. □

In fact, we have also proved that the group of symmetries of an octahedron is $S_4 \times C_2$: the octahedron is dual to the cube. Put each vertex of the octahedron on the centre of a face of the cube, and vice versa.



(Dodecahedron and Icosahedron are also dual, but they are not done here.)

Example: (Tetrahedron)
This is self-dual in the above sense. Let's number the vertices with $1, 2, 3, 4$.

Let G^+ be the group of rotations acting on vertices. We see that $\text{orb}(1) = \{1, 2, 3, 4\}$ and

$$\begin{aligned} \text{Stab}(1) &= \{\text{rotations in axis through 1 and centre of opposite side}\} \\ &= \{e,\ \text{rotation by } \frac{2\pi}{3},\ \text{rotation by } \frac{4\pi}{3}\}. \end{aligned}$$

So $|G^+| = 4 \cdot 3 = 12$ by Orbit-Stabiliser.

The action gives a group homomorphism $\varphi\colon G^+ \longrightarrow S_4$. Clearly $\text{Ker}\,\varphi = \{e\}$ (if all four vertices are fixed, the whole tetrahedron is fixed). So G^+ is a subgroup of S_4 of order 12.

On this information we guess A_4. Are we right?

We get $(234), (243) \in \text{Stab}(1)$ as seen above. Similarly we have $(123), (132) \in \text{Stab}(4)$, $(124), (142) \in \text{Stab}(3)$, $(134), (143) \in \text{Stab}(2)$. So we have all 3-cycles.

Rotation in axes through opposite edge-midpoints give $(12)(34), (14)(23), (13)(24)$. So we have indeed $G^+ \cong A_4$.

"There is no rotation that fixes two vertices and swaps the other two."

Now we look at all symmetries G. We get $\phi\colon G \longrightarrow S_4$ with $\text{Ker}\,\phi = \{e\}$. The reflection in the plane through 1 and 2 swaps $3, 4$, etc., so now $\text{Stab}(1) = \langle (234), (34) \rangle \cong D_6$. Think of it as the symmetries of the triangle face opposite of 1. This gives $|G| = 4 \cdot 6 = 24$, so as ϕ is an injection, we get $G \cong S_4$.

CHAPTER 6

Symmetric Groups Part II

Conjugacy classes in S_n

Recall: $\sigma, \tau \in S_n$ are conjugate if $\exists \rho \in S_n$ s.t. $\rho\sigma\rho^{-1} = \tau$. Ccls in S_n are very special.

56 Proposition: ("ccls in S_n are determined by cycle type")
Two elements of S_n are conjugate if and only if they have the same cycle type.

PROOF. If $(a_1 \ \cdots \ a_k)$ is a k-cycle and $\rho \in S_n$, then the conjugate $\rho(a_1 \ \cdots \ a_k)\rho^{-1}$ is the k-cycle $(\rho(a_1) \ \rho(a_2) \ \cdots \ \rho(a_k))$ because

$$\rho(a_1) \longmapsto a_1 \longmapsto a_2 \longmapsto \rho(a_2)$$
$$\rho(a_2) \longmapsto a_2 \longmapsto a_3 \longmapsto \rho(a_3) \text{ etc.}$$

If $\sigma = \sigma_1\sigma_2\cdots\sigma_l$ is a product of disjoint cycles, then $\rho\sigma\rho^{-1} = \rho\sigma_1\rho^{-1}\rho\sigma_2\rho^{-1}\cdots\rho\sigma_l\rho^{-1}$, so it has the same cycle type as σ.

Conversely, if σ, τ have the same cycle type, say

$$\sigma = (a_1 \ a_2 \ \cdots \ a_k)(a_{k+1} \ \cdots \ a_{k+l})\cdots$$
$$\tau = (b_1 \ b_2 \ \cdots \ b_k)(b_{k+1} \ \cdots \ b_{k+l})\cdots$$

then we use $\rho = \begin{pmatrix} a_1 & \cdots & a_{k+l} & \cdots & a_n \\ b_1 & \cdots & b_{k+l} & \cdots & b_n \end{pmatrix}$. Then $\rho\sigma\rho^{-1} = \tau$. So σ and τ are conjugate. □

We should do a sanity check: ρ really is a permutation because σ and τ are in disjoint cycle notation.

Example: Ccls of S_4

example element	cycle type	size of ccl	size of centraliser	sign
e	1111	1	24	+
(12)	211	6= $\frac{4\cdot3}{2}$	4	-
(12)(34)	22	3= $\frac{4\cdot3}{2\cdot2}$	8	+
(123)	31	8= $\frac{4\cdot3\cdot2}{3}$	3	+
(1234)	4	6= $\frac{4\cdot3\cdot2\cdot1}{4}$	4	-

The sizes of the centralisers are calculated using the Orbit-Stabiliser Theorem.

What can this tell us?
Recall: A normal subgroup is a union of ccls.

Example: Normal subgroups of S_4. They must contain e, the order must divide 24, they must be a union of ccls.

order 1	$\{e\}$
order 4	$\{e, (12)(34), (13)(24), (14)(23)\} = V_4 \cong C_2 \times C_2$.
	Check it really is a subgroup (Klein four group).
order 12	A_4 (kernel of signature)
order 24	S_4

So the quotients of S_4 (or homomorphic images) are:

$S_4/\{e\} = S_4$ $\quad$ $S_4/V_4 = \{V_4, (12)V_4, (13)V_4, (23)V_4, (123)V_4, (132)V_4\} \cong S_3 (\cong D_6)$

c.f. "groups of order 6" Proposition 35

$S_4/A_4 \cong C_2$ $\quad$ $S_4/S_4 \cong \{e\}$

Exercise: Repeat this for S_5.

Conjugacy in A_n

We have seen that $|S_n| = 2 \cdot |A_n|$ and that ccls in S_n are nice. What about ccls in A_n?
First thought:

$$\mathrm{ccl}_{S_n}(\sigma) = \{\tau \in S_n \mid \exists \rho \in S_n \text{ s.t. } \tau = \rho\sigma\rho^{-1}\}$$
$$\mathrm{ccl}_{A_n}(\sigma) = \{\tau \in A_n \mid \exists \rho \in A_n \text{ s.t. } \tau = \rho\sigma\rho^{-1}\}$$

Obviously $\mathrm{ccl}_{A_n}(\sigma) \subseteq \mathrm{ccl}_{S_n}(\sigma)$, as $A_n \subseteq S_n$. But it could be smaller.
E.g. (123) and (132) are conjugate in S_3 by (23), i.e. $(23)(123)(23) = (132)$. But $(23) \notin A_3$.
[BUT in S_5, also $(23)(45)(123)(23)(45) = (132)$!]
We use Orbit-Stabiliser:

$$|S_n| = |\mathrm{ccl}_{S_n}(\sigma)||C_{S_n}(\sigma)| \qquad \text{and}$$
$$|A_n| = |\mathrm{ccl}_{A_n}(\sigma)||C_{A_n}(\sigma)|$$

As $|A_n| = \frac{1}{2}|S_n|$, there are two options:

- ◇ *either* $\mathrm{ccl}_{S_n}(\sigma) = \mathrm{ccl}_{A_n}(\sigma)$ and $|C_{A_n}(\sigma)| = \frac{1}{2}|C_{S_n}(\sigma)|$
- ◇ *or* $\frac{1}{2}|\mathrm{ccl}_{S_n}(\sigma)| = |\mathrm{ccl}_{A_n}(\sigma)|$ and $C_{A_n}(\sigma) = C_{S_n}(\sigma)$.

Definition: When $|\mathrm{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\mathrm{ccl}_{S_n}(\sigma)|$, we say that the conjugacy class of σ **splits in** A_n.

When does this happen?
Note that ccls cannot split into more than two in A_n!
Recall: Any subgroup of S_n has either none or half of its elements odd (Proposition 22).

57 Proposition: ("splitting ccls")
For $\sigma \in A_n$, the ccl of σ splits in A_n if and only if no odd permutation commutes with σ.

Proof. We have $|\mathrm{ccl}_{A_n}(\sigma)| = \frac{1}{2}|\mathrm{ccl}_{S_n}(\sigma)|$ if and only if $C_{A_n}(\sigma) = C_{S_n}(\sigma)$. Clearly $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$, so this happens iff $C_{S_n}(\sigma) \subseteq A_n$, i.e. σ commutes with no odd permutation. □

Example: Ccls in A_4

example element	cycle type	$\lvert\mathrm{ccl}_{S_4}\rvert$	odd element in C_{S_4}?	$\lvert\mathrm{ccl}_{A_4}\rvert$
e	1111	1	yes, e.g. (12)	1
(12)(34)	22	3	yes, e.g. (12)	3
(123)	31	8	no: see below	4
				4

$C_{S_4}((123)) = \langle(123)\rangle$. See "ccls of S_4": the size is 3, and we know that definitely all powers of (123) commute with it, so that is everything.

Example: Ccls in A_5

example element	cycle type	$\lvert\mathrm{ccl}_{S_5}\rvert$	odd element in C_{S_5}?	$\lvert\mathrm{ccl}_{A_5}\rvert$
e	11111	1	yes, e.g. (12)	1
(12)(34)	221	15	yes, e.g. (12)	15
(123)	311	20	yes, e.g. (45)	20
(12345)	5	24	no: see below	12
				12

58 Lemma: $\sigma = (12345) \in S_5$ *has* $C_{S_5}(\sigma) = \langle\sigma\rangle$.

PROOF. We first find the size using Orbit-Stabiliser: $|\mathrm{ccl}_{S_5}(\sigma)| = 24$, $|S_5| = 120$, so $|C_{S_5}(\sigma)| = 5$. Clearly all powers of σ commute with σ, so $\langle\sigma\rangle \leqslant C_{S_5}(\sigma)$. But by sizes, $C_{S_5}(\sigma) = \langle\sigma\rangle$. □

59 Theorem: A_5 *is simple.*

PROOF. We know that normal subgroups must be unions of ccls, must contain e and their order must divide $|A_5| = 60$. The sizes of the ccls in A_5 are 1, 15, 20, 12, 12. But the only options of adding a subset of those including 1 to give a number which divides 60 is $1 = 1$ or $1 + 15 + 20 + 12 + 12 = 60$. So only $\{e\} \trianglelefteq A_5$ and $A_5 \trianglelefteq A_5$, so A_5 is simple. □

In fact, all A_n for $n \geqslant 5$ are simple (see GRM second year).

CHAPTER 7

Quaternions

Groups of order 8

60 Lemma: ("groups of order 8")
If G has order 8, then either:
G is abelian and isomorphic to one of C_8, $C_4 \times C_2$, $(C_2 \times C_2) \times C_2$, or
G is not abelian and isomorphic to one of D_8 or Q_8 (dihedral or quaternion).

Proof. If G contains an element of order 8, then $G \cong C_8$.

If all non-identity elements have order 2, then G is abelian (by Sheet 1, Q8). Let $a \neq b \in G \backslash \{e\}$. Then by the direct product theorem (Proposition 13, Chapter 1), $\langle a, b\rangle \cong \langle a\rangle \times \langle b\rangle$. Now take $c \in G \backslash \langle a, b\rangle$ (such a c must exist by sizes). Then again by the direct product theorem, $G \cong (\langle a\rangle \times \langle b\rangle) \times \langle c\rangle \cong C_2 \times C_2 \times C_2$.

So now assume G has no element of order 8, but there is an element $a \in G$ of order 4. Then $H = \langle a\rangle$ has index 2, so $H \trianglelefteq G$, and $G/H \cong C_2$ (by sizes). This means, for any $b \in G \backslash H$, bH generates G/H, with $(bH)^2 = b^2H = H$. So $b^2 \in \langle a\rangle$, and in particular b^2 commutes with a.

If $b^2 = a$ or a^3, then b has order 8, contradicting our assumption. So either $b^2 = e$ or $b^2 = a^2$. (This does not imply $b = a$.) Also $bab^{-1} = a^l$ for some l, since $\langle a\rangle \trianglelefteq G$.

Now $a = b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^lb^{-1} = (bab^{-1})^l = a^{l^2}$, where we use that b^2 commutes with a for the first step. So $l^2 \equiv 1 \pmod 4$, so $l \equiv \pm 1 \pmod 4$.

Cases:

- $l \equiv 1 \pmod 4$, i.e. $bab^{-1} = a$, so $ba = ab$, so G is abelian.
  - If $b^2 = e$, we have $G = \langle a, b\rangle \cong \langle a\rangle \times \langle b\rangle \cong C_4 \times C_2$ by the direct product theorem.
  - If $b^2 = a^2$, then $(ba^{-1})^2 = e$ (as G is abelian), and $G = \langle a, ba^{-1}\rangle \cong C_4 \times C_2$.
- $l \equiv -1 \pmod 4$, i.e. $bab^{-1} = a^{-1}$.
  - If $b^2 = e$, then $G = \langle a, b \mid a^4 = e = b^2, bab^{-1} = a^{-1}\rangle \cong D_8$, i.e. G is dihedral. (sizes help to make this entirely rigorous)
  - If $b^2 = a^2$, we potentially have a new group, called Q_8, the quaternions (see next section).

□

Why potentially? The relations could lead to a contradiction.
e.g. if $a^5 = e$, $b^2 = e$, then $bab = a^2 \Rightarrow a = b^2ab^{-2} = ba^2b^{-1} = (bab)^2 = a^4$, which is not true.

Quaternions

Definition: The set of matrices

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\}$$

forms a group under matrix multiplication, called the **quaternions** Q_8.

Exercise: Check it is a group. See next chapter: it is a subgroup of $\mathrm{GL}_2(\mathbb{C})$.

Remark: We know that this is not any of the other groups of order 8, because:

◇ it is not abelian:

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

◇ it is not dihedral: all elements except $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ have order 4.

We can check that taking $a = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ and $b = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, this group does indeed satisfy $a^4 = e$, $b^2 = a^2$ and $bab^{-1} = a^{-1}$.

Now that it exists, we could also write:

$$Q_8 = \langle a, b \mid a^4 = e, b^2 = a^2, bab^{-1} = a^{-1} \rangle$$

A nicer way to think of it:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with $(-1)^2 = 1$, $i^2 = j^2 = k^2 = -1$, $(-1)i = -i$ etc.
$ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$

We call it **anticommutative**.

Translation table:

1	-1	i	j	$k = ij$	$-i$	
e	$a^2 = b^2$	a	b	ab	$a^3 = ab^2 = b^2a$	
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$		

Complete it yourself as practice.

CHAPTER 8

Matrix groups

The general and special linear groups

Consider $M_{n\times n}(F)$, the set of $n\times n$ matrices over $F=\mathbb{R},\mathbb{C}$ (some field). Matrix multiplication is associative (e.g. as they represent functions), but not in general commutative. If we want I to be our identity, what matrices have inverses?

Definition:

$$\mathrm{GL}_n(F)=\{A\in M_{n\times n}(F)\mid A \text{ is invertibe}\}$$

is the **general linear group**.

61 Proposition: $\mathrm{GL}_n(F)$ *is a group.*

Proof. Check $\mathrm{GL}_n(\mathbb{R})$ or $\mathrm{GL}_n(\mathbb{C})$.
The identity is $\begin{pmatrix}1&&0\\&\ddots&\\0&&1\end{pmatrix}=I$, inverses are the inverse matrices, which exist by definition of $\mathrm{GL}_n(F)$, and the composite of invertible matrices is invertible (c.f. Lemma 6: the composite of bijective functions is bijective, or use $\det AB=\det A\det B$). Multiplication is associative. □

62 Proposition: ("det is a group hom")
$\det\colon \mathrm{GL}_n(F)\longrightarrow F\backslash\{0\}$ *is a surjective group homomorphism ($F=\mathbb{R}$ or $\mathbb{C}$).*

Proof. We know that $\det AB=\det A\det B$, so it is a group homomorphism. If A is invertible, then $\det A\neq 0$. Given $x\in F\backslash\{0\}$, $\det\begin{pmatrix}x&&0\\&\ddots&\\0&&1\end{pmatrix}=x$, so it is surjective. □

Definition: The kernel of det is the **special linear group**

$$\mathrm{SL}_n(F)=\{A\in\mathrm{GL}_n(F)\mid \det A=1\}.$$

So $\mathrm{SL}_n(F)\trianglelefteq\mathrm{GL}_n(F)$ as it is a kernel.

What is $\mathrm{GL}_n(F)/\mathrm{SL}_n(F)$? (Use the Isomorphism Theorem)
Note $Q_8\leqslant\mathrm{SL}_2(\mathbb{C})$.

Actions of $\mathrm{GL}_n(\mathbb{C})$

63 Proposition: $\mathrm{GL}_n(\mathbb{C})$ *acts faithfully on $\mathbb{C}^n$ by left multiplication, with two orbits.*

Proof. "applying the function to a vector".

- ◇ For $A\in\mathrm{GL}_n(\mathbb{C})$, $v\in\mathbb{C}^n$, we have $Av\in\mathbb{C}^n$.
- ◇ $Iv=v$ for all $v\in\mathbb{C}^n$.
- ◇ $A(Bv)=(AB)v$ for all $v\in\mathbb{C}^n$.

Intuitively, this action is clearly faithful as "only I acts as the identity".

Proper proof: a linear map is determined by what it does on a basis. Take the standard basis

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Any matrix which maps each e_k to itself must be I.

Orbits: clearly $A0 = 0$ for all $A \in \mathrm{GL}_n(\mathbb{C})$. Also, as A is invertible, $Av = 0 \Leftrightarrow v = 0$. So 0 forms a singleton orbit. Given any two vectors $v \neq w \in \mathbb{C}^n \backslash \{0\}$, there is a matrix $A \in \mathrm{GL}_n(\mathbb{C})$ s.t. $Av = w$. (Prove it with methods from V+M.) □

Similarly $\mathrm{GL}_n(\mathbb{R})$ acts on $\mathbb{R}^n$.

Exercise: Letting $\mathrm{SL}_n(\mathbb{C})$ act on $\mathbb{C}^n$, what orbits do you get?

64 Proposition: $\mathrm{GL}_n(\mathbb{C})$ *acts on* $M_{n\times n}(\mathbb{C})$ *by conjugation.*

Proof. Let $A \in M_{n\times n}(\mathbb{C})$, $P \in \mathrm{GL}_n(\mathbb{C})$. Then $PAP^{-1} \in M_{n\times n}(\mathbb{C})$, $IAI^{-1} = A$, and $(PQ)A(PQ)^{-1} = P(QAQ^{-1})P^{-1}$. □

How to think about this: matrices in $M_{n\times n}(\mathbb{C})$ represent maps $\mathbb{C}^n \longrightarrow \mathbb{C}^n$. Two matrices are conjugate if they represent the *same* map with respect to different bases. The P is then a base change matrix.

Special case $\mathrm{GL}_2(\mathbb{C})$ acting on $M_{2\times 2}(\mathbb{C})$:

We know from V+M that we have three different types of orbits: A is conjugate to a matrix of one of these forms:

- $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ with $\lambda \neq \mu$
- $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$
- $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$

C.f. V+M and eigenvectors. Also more generally Linear Algebra second year "Jordan Normal Form".

Orthogonal groups

Interlude: reminder from V+M:

A^T has entries $A^T_{ij} = A_{ji}$ "reflect in diagonal".

Facts:

- $(AB)^T = B^T A^T$
- $(A^{-1})^T = (A^T)^{-1}$
- $A^T A = A \Leftrightarrow AA^T = I \Leftrightarrow A^{-1} = A^T$
- $\det A^T = \det A$.

We are now most definitely in $\mathbb{R}$.

Definition: $O_n = O_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^T A = I\}$ is the **orthogonal group**.

We check it is a group: if $A, B \in O_n$, then $(AB)^T AB = B^T A^T AB = B^T IB = I$. Clearly $I^T = I$. If $A \in O_n$, then $A^T \in O_n$, because $(A^T)^T A^T = AA^T = I$. So $A^{-1} = A^T$ and we have inverses.

How to think of it: a matrix in O_n has ortho*normal* columns: for each column v, $v^T v = 1$ (normal), for different columns, $w^T v = 0$ (orthogonal). Such a matrix is called an orthogonal matrix, c.f. V+M.

65 Proposition: $\det\colon O_n \longrightarrow \{\pm 1\}$ *is a surjective group homomorphism.*

PROOF. For $A \in O_n$, we have $A^T A = I$, so $\det A^T A = (\det A)^2 = 1$, so $\det A = \pm 1$. We know $\det AB = \det A \det B$, and $\det \begin{pmatrix} -1 & & & \\ & 1 & & 0 \\ & & \ddots & \\ & 0 & & 1 \end{pmatrix} = -1$, so it is a surjective group homomorphism. □

Definition: The kernel of $\det\colon O_n \longrightarrow \{\pm 1\}$ is the **special orthogonal group**

$$SO_n = SO_n(\mathbb{R}) = \{A \in O_n \mid \det A = 1\}.$$

By the Isomorphism Theorem, $O_n/SO_n \cong C_2$.

66 Lemma: $O_n = SO_n \cup \begin{pmatrix} 1 & & & \\ & \ddots & & 0 \\ & & 1 & \\ & 0 & & -1 \end{pmatrix} SO_n$.

PROOF. Cosets partition the group (c.f. Lagrange, Theorem 23). □

67 Lemma: ("orthogonal matrices are isometries")
For $A \in O_n$ and $x, y \in \mathbb{R}^n$, we have
(1) $(Ax)^T(Ay) = x^T y$ *(A preserves dot product)*
(2) $|Ax| = |x|$ *(A preserves length)*

PROOF. $(Ax)^T(Ay) = x^T A^T A y = x^T I y = x^T y$ as $A^T A = I$. Then $|Ax|^2 = (Ax)^T(Ax) = x^T x = |x|^2$, so as both sides are positive, $|Ax| = |x|$. □

Note: orthogonal matrices are also linear maps, i.e. $0 \longmapsto 0$; not all isometries are linear. Isometries also form a group.

Rotations and reflections in 2 and 3 dimensions

Let's investigate $O_2(\mathbb{R})$ more closely.
Recall: $O_2 = SO_2 \cup \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) SO_2$.

68 Lemma: SO_2 *consists of all rotations of* $\mathbb{R}^2$ *around* 0.

PROOF. Let $A \in SO_2$, so $A^T A = I$ and $\det A = 1$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. So $A^T = A^{-1}$ implies $ad - bc = 1$, $c = -b$ and $d = a$. This gives $a^2 + c^2 = 1$, so set $a = \cos\theta = d$, $c = \sin\theta = -b$. So $A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. What does this map do to the standard basis?

$A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$ and $A \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$, so A is rotation by θ. (See diagram in lectures.)

Any rotation in $\mathbb{R}^2$ has this form, and so is in SO_2. □

69 Corollary: *Any matrix in* O_2 *is a rotation around* 0 *or a reflection in a line through* 0.

PROOF. If $A \in SO_2$, then A is a rotation as above. Otherwise,

$$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \text{for some } \theta \text{ (by Lemma 66)}$$
$$= \begin{pmatrix} \cos\theta & -\sin\theta \\ -\sin\theta & -\cos\theta \end{pmatrix}$$

This has eigenvalues $1, -1$, so it is a reflection (in the line which is the 1-eigenspace). The line goes through 0 because it is a linear map. □

Now we look at three dimensions.

70 Lemma: *Every matrix in SO_3 is a rotation around some axis.*

PROOF. Let $A \in SO_3$. Then $\det A = 1$, and A is an isometry (by Lemma 67), so the eigenvalues λ satisfy $|\lambda| = 1$ and multiply to 1. So

either $\exists$ complex eigenvalues $\lambda, \overline{\lambda}$ with $\lambda\overline{\lambda} = 1$, so the third eigenvalue is real and is $+1$,

or all eigenvalues are real and multiply to 1, so they are $1, 1, 1$ or $-1, -1, 1$.

So we can pick an eigenvector for eigenvalue 1 as the third basis vector, and then in some orthonormal basis we have

$$A = \begin{pmatrix} A' & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & 1 \end{pmatrix}.$$

Now A' is in $\mathbb{R}^2$ with $\det A' = 1$, and A' is still orthogonal, so $A' \in SO_2$, so by Lemma 68, A' is a rotation and

$$A = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

in some basis. □

71 Lemma: *Every matrix in O_3 is the product of at most three reflections (in planes through 0).*

PROOF. Recall $O_3 = SO_3 \cup \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right) SO_3$.

So if $A \in SO_3$, we know $A = \left(\begin{smallmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ in some basis, which is

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ -\sin\theta & -\cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

the product of two reflections.

If $A \in \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right) SO_3$, then it is the product of three reflections. □

Note: $\left(\begin{smallmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right) \in O_3$ needs the three reflections, as it is itself not a reflection in a plane.

Exercise: Think about these statements geometrically. C.f. Beardon 11.2 Orthogonal maps and 11.3.3.

Unitary groups

We can think of this as the "complex equivalent of orthogonal".

We use dagger: $(A^\dagger)_{ij} = \overline{A}_{ji}$

We still have:

- $(AB)^\dagger = B^\dagger A^\dagger$
- $(A^{-1})^\dagger = (A^\dagger)^{-1}$

- $A^\dagger A = I \Leftrightarrow AA^\dagger = I \Leftrightarrow A^{-1} = A^\dagger$
- $\det A^\dagger = \overline{\det A}$

Definition: $U_n = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^\dagger A = I\}$ is the **unitary group** (the group of all unitary matrices, also written $U(n)$).

Exercise: Check it is a group.

72 Lemma: $\det\colon U_n \longrightarrow S^1$ *is a surjective group homomorphism.*

Proof. Recall that S^1 is the unit circle, here viewed as a subgroup of the complex numbers. $1 = \det A^\dagger A = |\det A|^2$, so $|\det A| = 1$, so $\det A \in S^1$. $\det AB = \det A \det B$ as before, so it is a group homomorphism. Given $\lambda \in S^1$, we have $\begin{pmatrix} \lambda & & \\ & 1 & 0 \\ & 0 & \ddots \\ & & & 1 \end{pmatrix} \in U_n$ with determinant λ, so it is surjective. □

Definition: The kernel of $\det\colon U_n \longrightarrow S^1$ is SU_n, the **special unitary group**.

Note: in fact $Q_8 \leqslant SU_2$.
Unitary matrices preserve **complex dot product**:

$$x^\dagger y = (Ax)^\dagger (Ay)$$

where $x^\dagger y = \overline{x_1} y_1 + \overline{x_2} y_2 + \cdots + \overline{x_n} y_n$.

CHAPTER 9

Möbius group

Möbius maps

We want to study maps $f\colon \mathbb{C} \longrightarrow \mathbb{C}$ with $f(z) = \frac{az+b}{cz+d}$, $a, b, c, d \in \mathbb{C}$, $ad - bc \neq 0$.
Why $ad - bc \neq 0$?

$$\begin{aligned} f(z) - f(w) &= \frac{(ac + b(cw + d) - (aw + b)(cz + d)}{(cw + d)(cz + d)} \\ &= \frac{(ad - bc)(z - w)}{(cw + d)(cz + d)} \qquad \text{for all } z, w \in \mathbb{C} \end{aligned}$$

So if $ad - bc = 0$, then f is constant.

If $c \neq 0$, what about $f(-\frac{d}{c})$? Is it not defined?

We add a new point, ∞, to $\mathbb{C}$, to form the extended complex plane $C \cup \{\infty\} = \mathbb{C}_\infty$.

Construction: (Stereographic Projection)
Take the unit sphere, cut it in the equator with the complex plane. Take a rod attached to the north pole. Then the intersection points of the rod with the complex plane correspond to intersection points of the rod with the sphere. The north pole corresponds to ∞.

[$\mathbb{C}_\infty$ is called the **one-point compactification of** $\mathbb{C}$ (because it is compact, c.f. Met and Top in Easter).]

We call this sphere the **Riemann sphere**.

Definition: A **Möbius map** is a map $f\colon \mathbb{C}_\infty \longrightarrow C_\infty$ of the form $f(z) = \frac{az+b}{cz+d}$, with $a, b, c, d \in \mathbb{C}$, $ad - bc \neq 0$, with $f(-\frac{d}{c}) = \infty$ and $f(\infty) = \frac{a}{c}$ (if $c \neq 0$).

[For $c = 0$, $f(\infty) = \infty$.]

73 Lemma: *Möbius maps are bijections* $\mathbb{C}_\infty \longrightarrow \mathbb{C}_\infty$.

Proof. Note that $f(z) - f(w)$ shows that any Möbius map is injective on $\mathbb{C}$. The inverse of $f(z) = \frac{az+b}{cz+d}$ is $g(z) = \frac{dz-b}{-cz+a}$. Check the composition both ways. For example, for $z \neq \infty, z \neq \frac{a}{c}$ we have

$$f(g(z)) = \frac{a\left(\frac{dz-b}{-cz+a}\right) + b}{c\left(\frac{dz-b}{-cz+a}\right) + d} = \frac{adz - ab - bcz + ab}{cdz - cb - cdz + ad} = \frac{(ad - bc)z}{ad - bc} = z$$

Special cases: $f(g(\infty)) = f(-\frac{d}{c}) = \infty$ and $f(g(\frac{a}{c})) = f(\infty) = \frac{a}{c}$. (For $c = 0$: $f(g(\infty)) = f(\infty) = \infty$.)

Similarly $g \circ f = 1_{\mathbb{C}_\infty}$. □

74 Proposition: (Möbius group)
The Möbius maps form a group M under composition.

Proof. ◇ If $f_1(z) = \frac{a_1 z+b_1}{c_1 z+d_1}$, $f_2(z) = \frac{a_2 z+b_2}{c_2 z+d_2}$ with $a_i d_i - b_i c_i \neq 0$, then

$$f_2 \circ f_1(z) = \frac{a_2 \frac{a_1 z+b_1}{c_1 z+d_1} + b_2}{c_2 \frac{a_1 z+b_1}{c_1 z+d_1} + d_2} = \frac{(a_1 a_2 + b_2 c_1)z + (a_2 b_1 + b_2 d_1)}{(c_2 a_1 + d_2 c_1)z + (c_2 b_1 + d_1 d_2)} = \frac{a_3 z + b_3}{c_3 z + d_3}$$

with $a_3d_3 - b_3c_3 = (a_1a_2 + b_2c_1)(c_2b_1 + d_1d + 2) - (a_2b_1 + b_2d_1)(c_2a_1 + d_2c_1) = (a_1d_1 - b_1c_1)(a_2d_2 - b_2c_2) \neq 0$. This works for $z \neq \infty$, $z \neq -\frac{d_1}{c_1}$.

Again we need to check some special cases:

- $f_1(-\frac{d_1}{c_1}) = \infty$, $f_2(\infty) = \frac{a_2}{c_2}$. We check $f_2 \circ f_1(-\frac{d_1}{c_1}) = \frac{(a_1a_2+b_2c_1)(-\frac{d_1}{c_1})+a_2b_1+b_2d_1}{(c_2a_1+d_2c_1)(-\frac{d_1}{c_1})+c_2b_1+d_1d_2} = \frac{a_2(c_1b_1-a_1d_1)}{c_2(b_1c_1-a_1d_1)} = \frac{a_2}{c_2}$.
- $f_1(\infty) = \frac{a_1}{c_1}$, $f_2(\frac{a_1}{c_1}) = \frac{a_1a_2+b_2c_1}{c_2a_1+d_2c_1} = \frac{a_3}{c_3} = f_2 \circ f_1(\infty)$.

We possibly also have to check that for the z which f_1 sends to $-\frac{d_2}{c_2}$, it also works. (When $c_1 = 0$ or $c_2 = 0$, it is also easy to check.)

So indeed $f_2 \circ f_1$ is a Möbius map.

- $1_{\mathbb{C}_\infty} : \mathbb{C}_\infty \longrightarrow \mathbb{C}_\infty$ is $1(z) = \frac{1z+0}{0z+1}$ with $1 - 0 \neq 0$, so $1 \in M$.
- Inverses are $f^{-1}(z) = \frac{dz-b}{-cz+a}$ with $da - bc \neq 0$, so $f^{-1} \in M$. (check appropriate special cases)
- Composition of functions is alway associative.

□

Note: M is not abelian. For $f_1(z) = 2z$, $f_2(z) = z+1$ have $f_1 \circ f_2(z) = 2z+2$, $f_2 \circ f_1(z) = 2z+1$.

Remark: ("point at ∞ is not special")
"Morally", ∞ is no different to any other point on the Riemann Sphere. You can get quite far with the conventions "$\frac{1}{\infty} = 0$", "$\frac{1}{0} = \infty$" and "$\frac{a\infty}{c\infty} = \frac{a}{c}$"

Don't use these in other contexts, only on the Riemann Sphere!!!!

Clearly $\frac{az+b}{cz+d} = \frac{\lambda az+\lambda b}{\lambda cz+\lambda d}$ for any $\lambda \neq 0 \in \mathbb{C}$. So we don't have a "unique representation with a, b, c, d". (c.f. fractions $\frac{1}{2} = \frac{2}{4}$). But

75 Proposition: ("Möbius maps via matrices")
The map $\theta : \mathrm{GL}_2(\mathbb{C}) \longrightarrow M$ sending $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$ to f_A with $f_A(z) = \frac{az+b}{cz+d}$ is a surjective group homomorphism.

Proof. θ lands in M, as $A \in GL_2(\mathbb{C})$ gives $ad - bc \neq 0$. This also shows surjectivity. From previous calculations:

$$\theta(A_2)\theta(A_1)(z) = \frac{(a_1a_2 + b_2c_1)z + a_2b_1 + b_2d_1}{(c_2a_1 + d_2c_1)z + c_2b_1 + d_1d_2} = \theta(A_2A_1)(z).$$

□

The kernel of this θ is

$$\begin{aligned} \operatorname{Ker}\theta &= \{A \in \mathrm{GL}_2(\mathbb{C}) \mid z = \frac{az+b}{cz+d} \forall z\} \\ &= \{\lambda I \mid \lambda \in \mathbb{C}, \lambda \neq 0\} = Z. \end{aligned}$$

Here setting $z = \infty$ gives $c = 0$, then $z = 0 \Rightarrow b = 0$, and then $z = 1 \Rightarrow a = d$. We call the matrices λI **scalar matrices**. Z is the **centre** of $\mathrm{GL}_2(\mathbb{C})$: those matrices which commute with everything.

So by the Isomorphism Theorem: $M \cong \mathrm{GL}_2(\mathbb{C})/Z$.

Definition: $\mathrm{GL}_2(\mathbb{C})/Z = \mathrm{PGL}_2(\mathbb{C})$, the **projective general linear group**.

Remark: Using $f_A = f_B$ iff $B = \lambda A$ for some $\lambda \neq 0 \in \mathbb{C}$, we get $\theta|_{\mathrm{SL}_2(\mathbb{C})} : \mathrm{SL}_2(\mathbb{C}) \longrightarrow M$ also surjective, $\operatorname{Ker}(\theta|_{\mathrm{SL}_2(\mathbb{C})}) = \{\pm I\}$ (scalar matrices of determinant 1).

So also $M \cong \mathrm{SL}_2(\mathbb{C})/\{\pm I\} = \mathrm{PSL}_2(\mathbb{C})$.

"The Möbius group is isomorphic to the projective special linear group."

76 Proposition: ("geometry of Möbius maps")
Every Möbius map can be written as a composite of maps of the following form:

(i) $f(z) = az$, $a \neq 0$	***dilation/rotation***
(ii) $f(z) = z + b$	***translation***
(iii) $f(z) = \frac{1}{z}$	***combined inversion and reflection.***

PROOF. Let $g(z) = \frac{az+b}{cz+d} \in M$.

If $c = 0$, (i.e. $g(\infty) = \infty$): $g(z) = \frac{a}{d}z + \frac{b}{d}$, i.e. $z \xmapsto[(i)]{} \frac{a}{d}z \xmapsto[(ii)]{} \frac{a}{d}z + \frac{b}{d}$.

If $c \neq 0$, i.e. $g(\infty) = z_0 \in \mathbb{C}$ (note $z_0 = \frac{a}{c}$): Let $h(z) = \frac{1}{z-z_0}$, then $hg(\infty) = \infty$, so hg is of the above form. And $h^{-1}(w) = \frac{1}{w} + z_0$, which is a composite of type (iii) and (ii), so $g = h^{-1}hg$ is also a composite of maps of type (i), (ii) and (iii).

[Or direct calculation:

$$z \xmapsto[(ii)]{} z + \frac{d}{c} \xmapsto[(iii)]{} \frac{1}{z+\frac{d}{c}} \xmapsto[(i)]{} \frac{\frac{-ad+bc}{c^2}}{z+\frac{d}{c}} \xmapsto[(ii)]{} \frac{d}{c} + \frac{\frac{-ad+bc}{c^2}}{z+\frac{d}{c}} = \frac{az+b}{cz+d}\ ]$$ □

Exercise: The "non-calculation way" in the above proof can be transferred into another (different) composition (which of course has the same end result).

Fixed points

Any Möbius map with $c = 0$ fixes ∞, and $z \longmapsto z + 1$ only fixes ∞, whereas $z \longmapsto 2z$ also fixes 0. What can we say in general?

77 Proposition: *Any Möbius map with at least three fixed points is the identity.*

PROOF. Consider $f(z) = \frac{az+b}{cz+d}$. This has fixed points at those z which satisfy $\frac{az+b}{cz+d} = z \Leftrightarrow az + b = cz^2 + dz \Leftrightarrow cz^2 + (d-a)z - b = 0$. This quadratic has at most two roots, unless $c = b = 0$ and $d = a$, in which case f =identity. □

78 Proposition: ("Conjugacy classes of Möbius maps")
Any Möbius map is conjugate to $f(z) = \nu z$ for some $\nu \neq 0$, or to $f(z) = z + 1$.

PROOF. We have a surjective group homomorphism $\theta\colon \mathrm{GL}_2(\mathbb{C}) \longrightarrow M$ (see Prop. 75 "Möbius maps via matrices").

The ccls in $\mathrm{GL}_2(\mathbb{C})$ are of type

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \longmapsto g(z) = \frac{\lambda z + 0}{0z + \mu} = \frac{\lambda}{\mu}z \qquad \lambda, \mu \neq 0$$

$$\text{or} \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \longmapsto g(z) = z = 1 \cdot z \qquad \text{identity}$$

$$\text{or} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \longmapsto g(z) = \frac{\lambda z + 1}{\lambda} = z + \frac{1}{\lambda} \qquad \lambda \neq 0$$

But in fact $\begin{pmatrix} 1 & \frac{1}{\lambda} \\ 0 & 1 \end{pmatrix}$ is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$:

$$\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{\lambda} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\lambda} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \longmapsto g(z) = z + 1.$$

□

Now we see easily that (for $\nu \neq 0, 1$) νz has $0, \infty$ as fixed points, and $z + 1$ only ∞. Does this transfer to their conjugates?

79 Proposition: ("fixed points of Möbius maps")
Every non-identity Möbius map has exactly one or two fixed points.

PROOF. Given $f \in M$, $f \neq \mathrm{id}$, there is $h \in M$ s.t. $hfh^{-1}(z) = \nu z$ or $z+1$ (for $\nu \neq 0, 1$).

Now $f(w) = w \Leftrightarrow hfh^{-1}(h(w)) = h(w)$, so f and hfh^{-1} have the same number of fixed points (c.f. Sheet 4 Q9).

So f has either exactly 2 (for $hfh^{-1}(z) = \nu z, \nu \neq 0, 1$) or exactly 1 (for $hfh^{-1}(z) = z + 1$) fixed points. □

Permutation properties of Möbius maps

We have seen that any Möbius map with three fixed points is the identity.

80 Lemma: ("3-point determintation of Möbius maps")
Given $f, g \in M$, if there are $z_1, z_2, z_3 \in \mathbb{C}_\infty$ distinct such that $f(z_i) = g(z_i)$, then $f = g$.

PROOF. As Möbius maps are invertible, we have $g^{-1}f(z_i) = z_i$, so $g^{-1}f$ has three fixed points and is the identity (Prop. 77). So $g^{-1}f = \mathrm{id} \Rightarrow f = g$. □

So any Möbius map is determined by 3 points.

Definition: An action of G on X is called **three-transitive** if the induced action on the set $\{(x_1, x_2, x_3) \in X^3 \mid x_i \text{ pairwise distinct}\}$ given by $g(x_1, x_2, x_3) = (g(x_1), g(x_2), g(x_3))$ is transitive.

This means: for any two triples x_1, x_2, x_3 and y_1, y_2, y_3 of distinct elements of X, there is a $g \in G$ s.t. $g(x_i) = y_i$.

If this g is always unique, the action is called **sharply three-transitive**.

81 Proposition: *The Möbius group M acts sharply three-transitively on $\mathbb{C}_\infty$.*

PROOF. Given z_1, z_2, z_3 distinct, then

$$f(z) = \frac{z - z_2}{z - z_1} \frac{z_3 - z_1}{z_3 - z_2}$$

sends

$$\begin{aligned} z_1 &\longmapsto \infty \\ z_2 &\longmapsto 0 \\ z_3 &\longmapsto 1. \end{aligned}$$

Usual special cases:

$$\begin{aligned} &\text{If } z_1 = \infty \quad \text{then} \quad f(z) = \frac{z - z_2}{z_3 - z_2} \\ &\text{If } z_2 = \infty \quad \text{then} \quad f(z) = \frac{z_3 - z_1}{z - z_1} \\ &\text{If } z_3 = \infty \quad \text{then} \quad f(z) = \frac{z - z_2}{z - z_1}. \end{aligned}$$

Given also w_1, w_2, w_3 distinct in $\mathbb{C}_\infty$ and $g \in M$ sending

$$\begin{aligned} w_1 &\longmapsto \infty \\ w_2 &\longmapsto 0 \\ w_3 &\longmapsto 1, \end{aligned}$$

then we have $g^{-1}f(z_i) = w_i$.

By "3-point determination of Möbius maps" (Lemma 80) this $g^{-1}f$ is the unique Möbius map with that property. □

Three points also determine lines/circles.

We view a line in $\mathbb{C} \cong \mathbb{R}^2$ as a circle on the Riemann Sphere through ∞.

82 Lemma: ("equation of complex circle/straight line")
The general equation of a circle or straight line in $\mathbb{C}$ *is* $Az\overline{z} + \overline{B}z + B\overline{z} + C = 0$*, where* $A, C \in \mathbb{R}$*,* $|B|^2 > AC$*.*

PROOF. This comes from $|z - B| = r > 0$ for a circle and $|z - a| = |z - b|$ with $a \neq b$ for a straight line. C.f. V+M. □

Note: $A = 0$ gives a straight line. $A \neq 0, B = 0$ gives a circle centred at the origin. $C = 0$ gives a circle passing through the origin (radius=|centre|).

83 Proposition: *Möbius maps send circles/lines to circles/lines.*
Or: Möbius maps send circles on the Riemann Sphere to circles on the Riemann Sphere.

PROOF. Either: Calculate directly using $w = \frac{az+b}{cz+d} \Leftrightarrow z = \frac{dw-b}{-cw+a}$. Then $Az\overline{z} + \overline{B}z + B\overline{z} + C = 0 \Leftrightarrow A'w\overline{w} + \overline{B'}w + B'\overline{w} + C' = 0$ with $A', C' \in \mathbb{R}$.
Or: Use "geometry of Möbius maps" (Prop. 76) and check for each of the three types:
Dilation/rotation and translation are straight-forward.
$\frac{1}{z}$: Using $w = \frac{1}{z}$ we have $Az\overline{z} + \overline{B}z + B\overline{z} + C = 0 \Leftrightarrow Cw\overline{w} + Bw + \overline{B}\overline{w} + A = 0$ □

Example: Consider $f(z) = \frac{z-i}{z+i}$. Where does the real line go?
Real line = circle containing $\infty, 0, 1$. f maps this to the circle containing $f(\infty) = 1$, $f(0) = -1$, $f(1) = -i$. So to the unit circle.
The upper half plane goes to the inside (as $f(i) = 0$).
"Complementary components are mapped to complementary components."
In lectures I will add a diagram.

Cross ratio

Recall: Given distinct $z_1, z_2, z_3 \in \mathbb{C}_\infty$, there exists a unique $g \in M$ such that $g(z_1) = \infty$, $g(z_2) = 0$, $g(z_3) = 1$.

Definition: Given four distinct points $z_1, z_2, z_3, z_4 \in \mathbb{C}_\infty$, their **cross ratio** is $[z_1, z_2, z_3, z_4] = g(z_4)$ for g as above.

So $[\infty, 0, 1, \lambda] = \lambda$ (for any $\lambda \neq 0, 1, \infty$).
We know this exists and is uniquely defined because M acts sharply three-transitively on $\mathbb{C}_\infty$ (Prop. 81).
Note that different authors use different permutations of $1, 2, 3, 4$. (This doesn't matter as long as you are consistent.) Beardon is different to the one I've given.
Formula:

$$[z_1, z_2, z_3, z_4] = \frac{z_4 - z_2}{z_4 - z_1} \cdot \frac{z_3 - z_1}{z_3 - z_2}$$

with special cases as in Prop. 81.

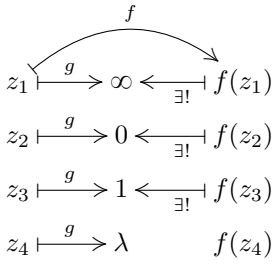
84 Lemma: ("double transpositions fix cross-ratio")
For z_1, z_2, z_3, z_4 *distinct points in* $\mathbb{C}_\infty$*, we have* $[z_1, z_2, z_3, z_4] = [z_2, z_1, z_4, z_3] = [z_3, z_4, z_1, z_2] = [z_4, z_3, z_2, z_1]$.

PROOF. By inspection of formula. □

So ours is the same as the one on Wikipedia.

85 Proposition: ("Möbius maps preserve cross-ratio")
If $f \in M$*, then* $[z_1, z_2, z_3, z_4] = [f(z_1), f(z_2), f(z_3), f(z_4)]$.

PROOF. Let g be the unique Möbius map s.t. $[z_1, z_2, z_3, z_4] = g(z_4) = \lambda$.



We know that there is a unique Möbius map with similar properties for the $f(z_i)$. But gf^{-1} has this property, so is the unique map. So $[f(z_1), f(z_2), f(z_3), f(z_4)] = gf^{-1}(f(z_4)) = g(z_4) = \lambda$. □

In fact, we see from this proof:

Given z_1, z_2, z_3, z_4 distinct and w_1, w_2, w_3, w_4 distinct in $\mathbb{C}_\infty$, there is $f \in M$ with $f(z_i) = w_i$ iff $[z_1, z_2, z_3, z_4] = [w_1, w_2, w_3, w_4]$.

86 Corollary: *The points z_1, z_2, z_3, z_4 lie on some circle or line iff $[z_1, z_2, z_3, z_4] \in \mathbb{R}$.*

PROOF. Let C be the circle/straight line through z_1, z_2, z_3. Let g be the unique Möbius map with $g(z_1) = \infty$, $g(z_2) = 0$, $g(z_3) = 1$ (c.f. Proposition 81). Then $g(z_4) = [\infty, 0, 1, g(z_4)] = [g^{-1}(\infty), g^{-1}(0), g^{-1}(1), g^{-1}(g(z_4))]$ (as Möbius maps preserve cross-ratio, Prop. 85), which in turn is equal to $[z_1, z_2, z_3, z_4]$. So $z_4 \in C \Leftrightarrow g(z_4) = [z_1, z_2, z_3, z_4] \in \mathbb{R}$, because Möbius maps send circle/lines to circles/lines (Prop. 83). □

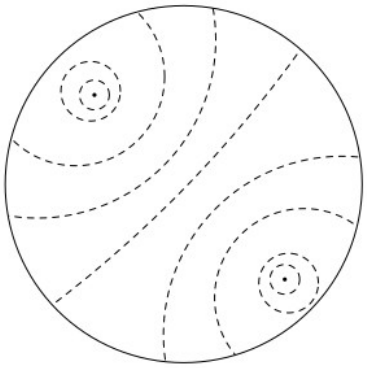
(Extra) Summary of conjugacy classes

Any non-identity Mbius map is conjugate to one of these four types:

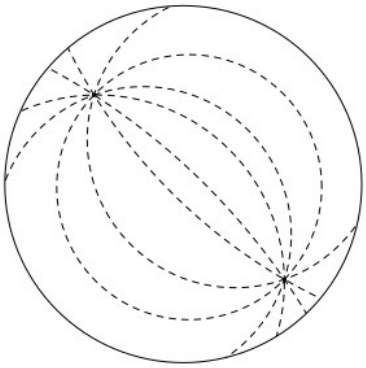
		Action on Riemann Sphere
Elliptic:	$f(z) = \nu z$ with $\lvert\nu\rvert = 1$ or $f(z) = e^{i\theta}z$	2 fixed points, other points move along circles round the fixed points
Hyperbolic:	$f(z) = \nu z$ with $\nu \in \mathbb{R}^+$, $\nu \neq 1$ or $f(z) = rz$, $r \in \mathbb{R}^+$, $r \neq 1$	2 fixed points, other points move on circular arcs from one fixed point to the other
Loxodromic:	$f(z) = \nu z$ with $\nu \notin \mathbb{R}^+$, $\lvert\nu\rvert \neq 1$ or $f(z) = re^{i\theta}z$	2 fixed points, other points move on spirals away from one fixed point towards the other
Parabolic:	$f(z) = z + 1$	1 fixed point, other points move on circles through the fixed point, away on one side, towards on the other

You can see the action on the Riemann sphere in the pictures below. These images are taken from T. K. Carne's lectures notes for Geometry and Groups, which can be found at

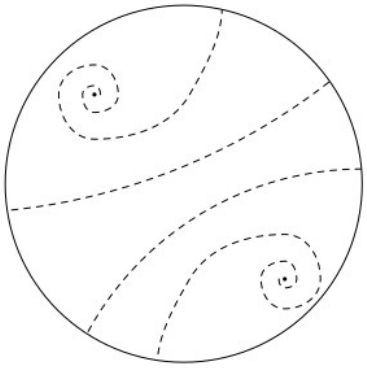
`www.dpmms.cam.ac.uk/~tkc/GeometryandGroups/GeometryandGroups.pdf`



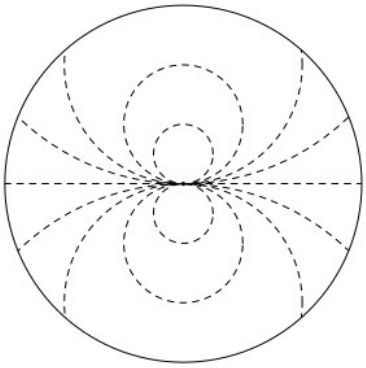
Elliptic



Hyperbolic



Loxodromic



Parabolic