Sets and Groups

Barry Monson, UNB

1 Sets

In the logical development of any branch of mathematics, each definition of a concept involves other concepts or relations. Thus, the only way to avoid a vicious circle is to accept certain *primitive concepts* or relations as undefined. Likewise, the proof of each proposition (or theorem) uses other propositions. Hence, to again avoid a vicious circle we must accept certain fundamental propositions – called *axioms* or *postulates* – as true but unproved. (Here I have paraphrased a particularly nice description due to H. S. M. Coxeter.)

Although the starting point for this process is somewhat arbitrary, most modern mathematicians begin with *set theory* and build up from there[1]. Keeping in mind the vicious circle, we realize that there is no point giving a formal definition of *set*. Instead, at the beginning, we can only discuss informal but sensible ways of thinking about sets[2]. Thus a set A is any collection of objects x, called *elements* of the set[3]. We write

$$x \in A$$

(and say 'x belongs to A' or 'x is an element of the set A) if indeed x is one of the objects in A. If the object y is not in A we write

$$y \notin A.$$

Intuitively, if $x \in A$, then x and A have 'different levels of organization'.

Example.

$$\begin{aligned} A &= \text{one of your classes last term} \\ x &= \text{you (or one of your classmates)} \\ y &= \text{George W. Bush} \end{aligned}$$

so $x \in A$, $y \notin A$. Again intuitively, the class A has a 'higher level of organization'. Now imagine that students drop the class one by one. The class A changes to B, then C, etc. as enrolment drops. We say B is a subset of A, C is a subset of B, indeed C is a subset of A:

[1] In practice, we aren't deterred by 20th century discoveries, due to Gödel and other logicians, that the axiomatic method has inevitable and surprising limitations. For example, any mathematics which accepts the legitimacy of the natural numbers 1, 2, 3, ... must contain theorems (i.e., true statements) which cannot be proved!

[2] The American mathematician Paul Halmos has written an excellent book 'Naive Set Theory', as an introduction to the foundations of mathematics for working mathematicians.

[3] To repeat: this is a way of thinking, not a precise definition.

$$C \subseteq B \subseteq A.$$

The sets $A,\ B,\ C, \ldots$ are different but still have the 'same level of organization'. We can image that everyone drops the class, so it makes sense to allow an empty class E, still satisfying

$$E \subseteq A.$$

If we try to make a census of all elements x of A, we might ask 'Which of you were born in Fredericton?' or 'Which of you are Math. majors?' or 'Which of you have blond hair?', etc. We wouldn't count twice a person who answered yes to two or more questions. Thus, as is reasonable, we shall agree that:

'order and repetition are irrelevant when
assessing elements in a set'.

(If order and repetition are important, we instead employ a *list*, which is really a *function*, which is really a very special kind of set! See below.)

Definitions. Suppose $A,\ B$, etc. are sets.

1. A is a *subset* of B, written $A \subseteq B$, if every element of A is an element of B:

$$x \in A \Rightarrow x \in B.$$

2. A *equals* B, written $A = B$, if $A \subseteq B$ and $B \subseteq A$:

$$\begin{aligned} x \in A &\Rightarrow x \in B \\ x \in B &\Rightarrow x \in A \end{aligned}$$

   In brief, $x \in B$ if and only if $x \in A$. Intuitively, A and B have the same elements.

3. An *empty set* E has no elements.

Axioms. This isn't a course in set theory, so we won't say much. Instead, a sensible approach is to learn the material informally through examples and by proving simple theorems, sort of ignoring the axioms.

But we do note that in order to avoid paradoxes we must insist that

$$x \in x$$

is a meaningless statement for any mathematical object x. Intuitively, x cannot be an element of itself, because it would then simultaneously have two different levels of organization. However,

$$x \in \{x\}$$

is always true; and

$$x \subseteq x$$

is also perfectly okay, so long as x itself is a set.

Theorem. The empty set is unique: if E and E' are empty sets, then $E = E'$.

Proof. Convince yourself. □

Notation. When an interesting object is shown to be uniquely specified, it often deserves a special notation. The empty set is denoted

$$\emptyset \, .$$

Exercise. For any set A whatsoever, prove that

$$\emptyset \subseteq A \, .$$

More Definitions.

4. The *union* of two sets $A,\ B$ is the set of all objects in either A or B (or both):

$$A \cup B = \{x : x \in A \ \text{ or } \ x \in B\}.$$

5. The *intersection* of sets $A,\ B$ is the set of all objects in both A and B:

$$A \cap B = \{x : x \in A \ \text{ and } \ x \in B\}.$$

6. Sets A and B are *disjoint* if $A \cap B = \emptyset$.

Remark. There are similar definitions for any finite family of sets

$$A_1 \cup \ldots \cup A_k \quad \text{or} \quad A_1 \cap \ldots \cap A_k,$$

or even any indexed family of sets A_t, where $t \in \mathcal{I}$. The indexing set $\mathcal{I}$ could be infinite. In general then, we write

$$\bigcup_{t\in\mathcal{I}} A_t \quad \text{or} \quad \bigcap_{t\in\mathcal{I}} A_t.$$

***

Sometimes we can explicitly enumerate the elements of a set, as in

$$A = \{5, 6, 7\},$$

or even in

$$\mathbb{S} = \{1, 4, 9, 16, \ldots\}.$$

(The use of "..." assumes the pattern is clear.) Maybe an explicit description is better as in

$$\mathbb{S} = \{n \in \mathbb{N} : \ n = a^2, \ \text{ for some } \ a \in \mathbb{N}\}.$$

Thus $\mathbb{S}$ is a subset of the natural numbers $\mathbb{N}$.

Exercises.

1. Let $A = \{2, \{1\}\}, \ \ B = \{\{\emptyset, \{3\}\}\}$.
   (a) What are the elements of A?
   (b) What is the cardinality of A (number of distinct elements)?
   (c) What are the distinct elements of B? What is its cardinality?
2. (a) What is cardinality of $\emptyset$?
   (b) Of $\{\emptyset\}$?
   (c) Of $\{\emptyset, \{\emptyset\}\}$?
3. We know $\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z}^{\geq} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. How many subset relations of the form $A \subseteq B$ are there between these sets? Give the standard names for each of these sets.

4. Let

$$\begin{aligned} A &= \{5, 6, 7\} \\ B &= \{5, 7\} \\ C &= \{6, 6, 5, 7, 5, 7\} \end{aligned}$$

True or False:

$$\begin{aligned} A &= B \_\_\_\_\_ \\ A &= C \_\_\_\_\_ \\ C &\subseteq A \_\_\_\_\_ \\ C &\subseteq B \_\_\_\_\_ \\ B &\subseteq A \_\_\_\_\_ \\ B &\neq A \_\_\_\_\_ \\ B &\in A \_\_\_\_\_ \\ A &\subseteq A \_\_\_\_\_ \\ \{6\} &\subseteq A \_\_\_\_\_ \\ \{6\} &\in A \_\_\_\_\_ \\ 6 &\subseteq A \_\_\_\_\_ \\ 6 &\in A \_\_\_\_\_ \\ \emptyset &\subseteq A \_\_\_\_\_ \\ \emptyset &\in A \_\_\_\_\_ \end{aligned}$$

5. Is it possible that

$$x \in A \quad \text{and} \quad x \subseteq A$$

are both true?

6. Find out what the subset lattice of a set A is and sketch it, when $A = \{1, 2, 3\}$.

Definitions. If a set A comes with an operation, say "+", then we can 'add' subsets of A. Suppose $B \subseteq A$ and $C \subseteq A$ (two subsets of A). Then by definition

$$B + C := \{x + y : x \in B \text{ and } y \in C\}.$$

The sets $B,\ C$ could be finite or infinite. In particular, B could be a singleton (cardinality 1), say

$$B = \{b\}.$$

Then instead of $\{b\} + C$ we write $b + C$ for more pleasant reading.

Similarly, if set A comes equipped with a multiplication "$\times$", we might suppress the operation:

$$\begin{aligned} BC &:= \{xy : x \in B \text{ and } y \in C\} \\ bC &:= \{by : y \in C\}. \end{aligned}$$

Exercises (Continued).

6. Describe, say by a 'clearly understood' listing, these subsets of the integers $\mathbb{Z}$.

   (a) $3\mathbb{Z}$

   (b) $1 + 2\mathbb{Z}$

   (c) $12\mathbb{Z} + 21\mathbb{Z}$

   (d) For specific positive integers $a,\ b$, what is $a\mathbb{Z} + b\mathbb{Z}$ in general?

7. Describe these subsets of the reals $\mathbb{R}$:

   (a) $\mathbb{Z} \cap (\sqrt{2}\mathbb{Z})$.

8. Euclidean Geometry.

   A typical triangle will be denoted $\triangle ABC$. For simplicity, let A, B, C denote the angles and let a, b, c be the lengths of the opposite edges. Let

   $$\begin{aligned} U &= \{\triangle ABC : C = 90^\circ\} \\ V &= \{\triangle ABC : a^2 + b^2 = c^2\} \end{aligned}$$

   In fact $U = V$.

   (a) Rephrase $U \subseteq V$ as a geometrical theorem. What is its conventional name?

   (b) Restate $V \subseteq U$ as such a theorem. (This is the *converse* to the theorem in (a).)

(c) Restate $U = V$ using 'if and only if' lingo. Using 'necessary and sufficient' lingo.

9. In a vector space, like

$$\mathbb{R}^2 = \{\vec{u} = [x, y] : x \in \mathbb{R},\ y \in \mathbb{R}\}$$

we have two operations:

$$\begin{aligned} \vec{u_1} + \vec{u_2} &= [x_1, y_1] + [x_2, y_2] := [x_1 + x_2, y_1 + y_2] \\ t\vec{u} &= t[x, y] := [tx, ty] \end{aligned}$$

(component-wise addition and scalar multiplication, for scalars $t \in \mathbb{R}$).

Give geometrical descriptions for

(a) $\mathbb{R}[2, 1]$ (strictly speaking, we here mean $\mathbb{R}\{[2, 1]\}$)

(b) $[-1, 1] + \mathbb{R}[2, 1]$

(c) $\mathbb{Z}[1, 0] + \mathbb{Z}[0, 1]$

(d) $\mathbb{Z}[1, 0] + \mathbb{Z}\left[-\frac{1}{2}, \frac{\sqrt{3}}{2}\right]$

(e) $\{[x, y] : x \in \mathbb{Z} \text{ and } y \in \mathbb{Z}\}$

(f) $\{[x, y] : x \in \mathbb{Z} \text{ or } y \in \mathbb{Z}\}$

Definition. For any two sets A, B, the (*Cartesian*) *product* $A \times B$ is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$:

$$A \times B := \{(a, b) : a \in A, b \in B\} .$$

Example.

$$\{0, 1\} \times \{x, y, z\} = \{(0, x), (0, y), (0, z), (1, x), (1, y), (1, z)\} .$$

Similarly,

$$A_1 \times \cdots \times A_n$$

is the set of all *ordered* n-tuples $(a_1, \ldots, a_n)$ with $a_j \in A_j$, $1 \leqslant j \leqslant n$. In the special case that all sets are the same, say $A = A_1 = \ldots = A_n$, we often write A^n instead.

Example.

$$\mathbb{R}^2 = \{\, [x_1, x_2] \,:\, x_1, x_2 \in \mathbb{R}\} .$$

(The square brackets are commonly used as a visual reminder that the ordered pair is to be treated as a vector.)

Definition. A *relation* $\mathcal{R}$ from a set A to a set B is merely any subset of $A \times B$:

$$\mathcal{R} \subseteq A \times B$$

To indicate that $(a, b) \in \mathcal{R}$ we write

$$a \mathcal{R} b .$$

As we shall see below, a *function* $f : A \to B$ is a very special sort of relation.

Very often we have $A = B$; extremely useful relations in this case are *equivalence relations* and *partial orders* on A.

Exercises. Using this rather abstract point of view, analyze the following familiar relations.

(a) The usual *total order* '$<$' on the reals $\mathbb{R}$ can be defined as follows:

$$< \;:=\; \{(x, y) \in \mathbb{R}^2 : y - x \text{ is positive.}\}$$

(Presumably in constructing the reals we have somewhere been told which of them are 'positive'). Sketch $<$ as a subset of $\mathbb{R}^2$.

(b) On the positive integers $\mathbb{N}$ define the usual *divisibility* relation '$|$' by $a|b$ if a divides b (without remainder).

Sketch $|$ as a subset of $\mathbb{N}^2$ (itself a subset of $\mathbb{R}^2$).

2 Functions

1. **Definitions**. Let X, Y be two sets, finite or infinite. A *function* f is any rule[4] which associates to each element x in X exactly one element, denoted $f(x)$, in Y. In brief, we write

$$f : X \to Y \ .$$

The set X is the *domain* of f.

Note that the *range*

$$f(X) := \{f(x) \,|\, x \in X\}$$

could be a *proper* subset of Y. If in fact $f(X) = Y$, then we say f is *onto* or *surjective*.

If f maps distinct inputs to distinct outputs, i.e.

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \ ,$$

then we say that f is $1-1$ (or *injective*). In contrapositive fashion, we could equivalently say that

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \ .$$

Example. It is useful to consider the airplane booking function f from the passenger set X on a particular flight to the seat set Y on the airplane: $f(x)$ is the seat occupied by person x, for each passenger $x \in X$. Thus, f onto means that every seat is filled, and f $1-1$ means that no two people are assigned the same seat (the flight is not stupidly booked). Clearly, if both conditions hold, there is exactly one seat for each passenger; in other words, the number of seats is the same as the number of passengers. Note that you could 'see this' by simply looking at the cabin, without counting or knowing the number of passengers or seats. These considerations motivate the following definitions and observations.

More Definitions. A function $f : X \to Y$ is *bijective* if it is both $1-1$ and onto.

We observe that the domain X and range Y must then have the same cardinality, even if both are infinite. Put otherwise, f defines a *1–1 correpondence* between the elements of X and the elements of Y. In this manner, by construction of suitable functions, we can assess whether certain infinite sets have or do not have the same 'number' of elements.

[4] If you object to the somewhat vague term 'rule', you should note that it is quite possible to give a very precise, but less intuitive definition: the function f is actually a subset of $X \times Y$, with the property that each $x \in X$ is the first entry in exactly one ordered pair $(x, y) \in f$. In other words, f is a special sort of relation from X to Y, so

$$f \subseteq X \times Y \ .$$

In fact, the set inclusion has to be proper here, unless Y has what cardinality?

Any bijection $f : X \to Y$ has an *inverse*

$$f^{-1} : Y \to X$$

defined by $f^{-1}(a) = b$ whenever $f(b) = a$, for $a \in Y, b \in X$. (Just unseat each passenger.)

2. **Exercises on Functions**

   (a) When $f : X \to Y$ is bijective, check that the above description of f^{-1} really does define a function. (You have to show that *for each $a \in Y$ there exists exactly one $b \in X$* such that $f(b) = a$.)
   Also check that f^{-1} is itself bijective, and that *its* inverse is f. This proves that

   $$(f^{-1})^{-1} = f \ .$$

   (b) Exhibit a bijection from the open real interval $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$ to $\mathbb{R}$ itself.

   (c) Exhibit a bijection between the the set $\mathbb{N}$ (of all natural numbers) and the proper subset $Y = \{2, 4, 6, 8, \ldots\}$ of just the even natural numbers.

   (d) If X is finite, say with n elements, how many bijections $f : X \to X$ are there? (Think: given n people in n chairs, how many ways can they rearrange themselves?)

3. **More Definitions**. The *identity function*

   $$1 : X \to X$$

   satisfies $1(x) = x$ for all $x \in X$. We write 1_X if we need to emphasize the domain X.

   Exercise. Prove that 1 is a bijection.

4. **Definition** Suppose $f : X \to Y$, $g : Y \to W$ are any functions. Then we define the *composite function*

   $$g \circ f : X \to W$$

   by $g \circ f(x) := g(f(x))$, for all $x \in X$.

   Remark. In certain contexts (but not first year calculus!), we write gf instead for the composite function.

   Exercises. (a) Convince yourself that this definition makes sense.

   (b) For $f : X \to Y$, prove that $f \circ 1_X = f = 1_Y \circ f$.

5. **Still More Exercises on Functions**. Suppose $f : X \to Y,\ g : Y \to W,\ h : W \to V$ are any functions, subject to varying requirements below. Prove that

   (a) In all cases
   $$(h \circ g) \circ f = h \circ (g \circ f)$$
   (both mapping what set to what set?). Thus composition is always *associative*, with no assumptions concerning 1-1 or onto.

   (b) If f, g are 1-1, so is $g \circ f$.

   (c) If f, g are onto, so is $g \circ f$.

   (d) If f, g are bijective, then so is
   $$g \circ f : X \to W.$$
   Thus, in this case there is an inverse
   $$(g \circ f)^{-1} : W \to X.$$
   Rewrite
   $$(g \circ f)^{-1} = \_\_\_\_\_.$$

   (e) Suppose $f : X \to Y,\ g : Y \to X$, no longer necessarily 1-1 or onto. Also suppose that
   $$f \circ g = 1_Y \ ,$$
   the identity function on Y. Prove that g is 1-1 and f is onto.

   (f) Suppose $f : X \to X$. Thus $f^2 := f \circ f$ is defined. More generally, for an integer $n \geqslant 1$, we write
   $$f^n := \underbrace{f \circ f \circ \ldots \circ f}_{\text{n repeats}}.$$
   (By the associativity mentioned earlier, this notation makes sense.)
   Now suppose $f^n = 1_X$ for some integer $n \geqslant 1$. Use the previous exercise to show that f has to be bijective; and write f^{-1} in another way.

3 Groups

A *group* is a set G equipped with a binary operation satisfying a few key properties. The operation is typically written $+, \times, *, \circ$, etc.

3.1 Binary Operations

The idea of a *binary operation* on a set G is that given $a, b \in G$ (allowing $a = b$) we can produce a new element

$$a * b \text{ (also in } G).$$

Remarks.

1. Think: apple * apple = apple; do you know any non-binary operations?
2. We emphasize that $a * b$ is *uniquely* given once a, b are known.
3. We typically must define $a * b$. So it is always crucial to check that arbitrary choices, if any, in calculations do not actually affect the final outcome $a * b$. In short, our description of $a * b$ must be *well-defined*.
4. Thus $*$ is really a function
$$* : G \times G \to G$$
5. Example.
$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.$$
We have $+(5, 3) = 8$, $+(3, -7) = -4$ and $+(-13, 0) = -13$. Of course, for brevity we usually write $a + b$ instead of $+(a, b)$.

3.2 Some Desirable Properties for the Operation (in a Group)

Let's return to a general group G; write $a * b$ for $a, b \in G$. Based on our experience with familiar examples, we want $a * b$ to have the following natural properties:

1. $(a * b) * c = a * (b * c)$, $\quad \forall a, b, c \in G$. (The operation $*$ is *associative*.)
2. There exists in G some special element e such that
$$e * a = a \qquad \text{for all } a \in G \ .$$
3. For each $a \in G$, there exists an element b (depending on a) such that
$$b * a = e \ ,$$
where e is an element mentioned in requirement (2).

Remarks:

1. Properties (1), (2), (3) for a binary operation $*$ on a set G actually define a group.

2. We do *not* assume $a * b = b * a$ always holds, though it may occasionally do so. For example, $a * a = a * a$ for all $a \in G$.

   In a *commutative* (or *abelian*) group G we do have

$$a * b = b * a \qquad \forall a, b \in G \; .$$

3.3 Some Little but Important Theorems for all Groups

Let $a, b... \in G$ be typical group elements. Let e be an element as defined in requirement (2) above.

1. **Theorem**. If for some $a \in G$ we have $a * a = a$, then $a = e$.
   Proof. By property (2) there exists a b such that $b * a = e$. Thus

$$\begin{aligned} e &= b * a \\ &= b * (a * a) \\ &= (b * a) * a \\ &= e * a \\ &= a \; . \end{aligned}$$

   □

2. **Theorem** Suppose $\tilde{e} \in G$ also satisfies $\tilde{e} * a = a$ for all $a \in G$. Then $\tilde{e} = e$.
   Proof. $\tilde{e} * \tilde{e} = \tilde{e}$, so $\tilde{e} = e$ by the preceding theorem. □

   Meaning. There is a *unique* element $e \in G$ such that

$$e * a = a \qquad \forall a \in G \; .$$

   Definition.: The unique element e is called the *identity* in G.

3. **Theorem**. If $b * a = e$, then $a * b = e$.

   Remark. Thus some commuting must happen.

   Proof.

$$\begin{aligned} (a * b) * (a * b) &= a * [b * (a * b)] \\ &= a * [(b * a) * b] \\ &= a * [e * b] \\ &= a * b \end{aligned}$$

   So, by the first theorem, $a * b = e$. □

4. The assumption in defining property (2) for groups is that $e * a = a, \qquad \forall a \in G$. Compare that with the following

   Theorem : $\qquad a * e = a \qquad \forall a \in G.$

   Remark: again this shows that a little more commuting is forced.

   Proof. By property (3), there exists an element $b \in G$ such that $b * a = e$. Thus

$$\begin{aligned} a * e &= a * (b * a) \\ &= (a * b) * a \\ &= e * a \\ &= a \ . \end{aligned}$$

   □

   Remark: The identity e thus commutes with all elements of G.

5. **Theorem** Given any $a \in G$, there exists *exactly one* element b such that $b * a = e$.

   Proof: Suppose that $b * a = e$ and $c * a = e$. From above we therefore have $a * b = e$ and $a * c = e$. So:

$$\begin{aligned} c * (a * b) &= c * e \\ (c * a) * b &= c \\ e * b &= c \\ b &= c \end{aligned}$$

   □

   Definition: The unique element guaranteed for each a by this theorem is called is the *inverse* of a, and is denoted a^{-1}. Thus we have already proved that

$$a * a^{-1} = a^{-1} * a = e \ .$$

6. **Theorem-Exercise** Guess and prove that $\forall a, b \in G$,

$$(a * b)^{-1} = \_\_\_\_\_ \ .$$

   Hint: if your guess for the inverse works, it must be the unique inverse.

3.4 Examples.

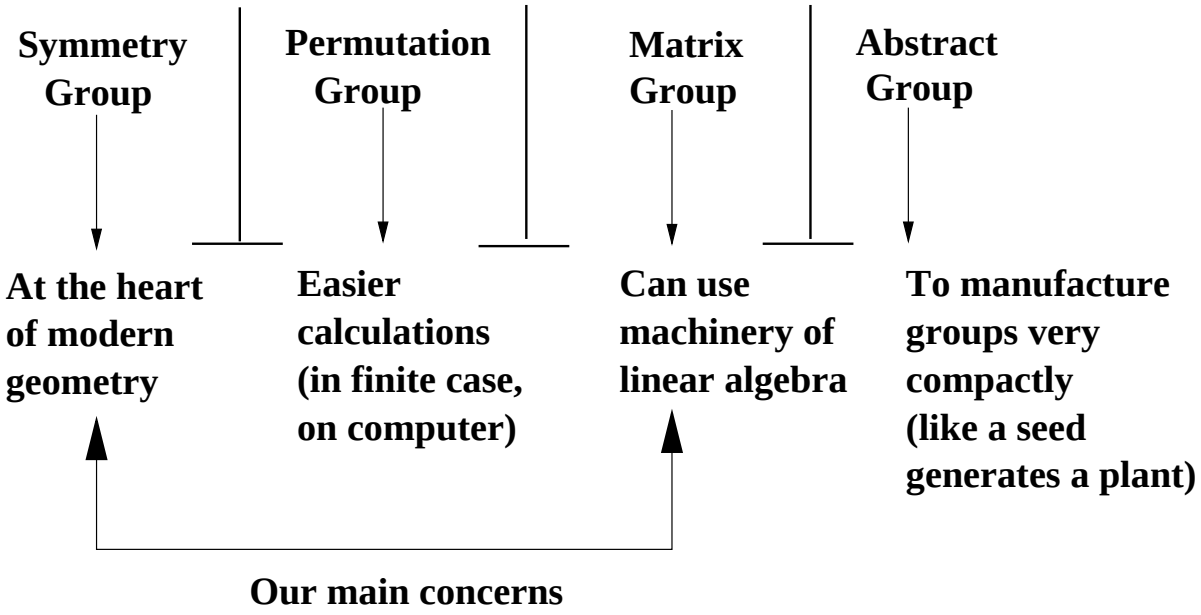
In each case, indicate whether the given set and operation do yield a group. If not, indicate which of properties (1), (2) or (3) fails. When you do obtain a group, clearly point out the identity and describe the inverse of each element a.

the set G	the operation $*$
$\mathbb{Z}$	$+$
$\mathbb{Z}$	$-$
$\mathbb{Z}$	$\cdot$
$\mathbb{Q}$	$+$
$\mathbb{R}$	$+$
$\mathbb{R}$	$-$
$\mathbb{C}$	$-$
$\mathbb{Q}^*$	$\cdot$
$\mathbb{M}_2(\mathbb{R})$	$+$
$\mathbb{M}_2(\mathbb{R})$	$\times$
$\{\pm 1\}$	$\cdot$
$\{1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\}$	$\cdot$
$C_n = \{e^{\frac{(2\pi i)k}{n}}, 0 \leqslant k \leqslant n-1\}$	$\cdot$

Note that $\mathbb{Q}^*$ denotes the non-zero rational numnbers. And $\mathbb{M}_2(\mathbb{R})$ is the collection of all 2×2 real matrices.

4 Isomorphic Approaches to the Same Group

It is often possible, and fruitful, to look at one and the same group from several points of view:



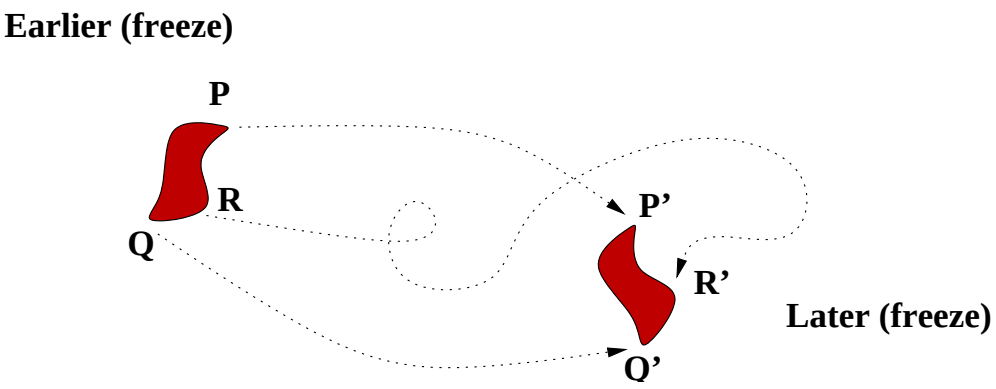
In geometry, the idea of *symmetry* is crucial. The parallel idea in algebra is the *matrix group*.

5 Motion and Symmetry

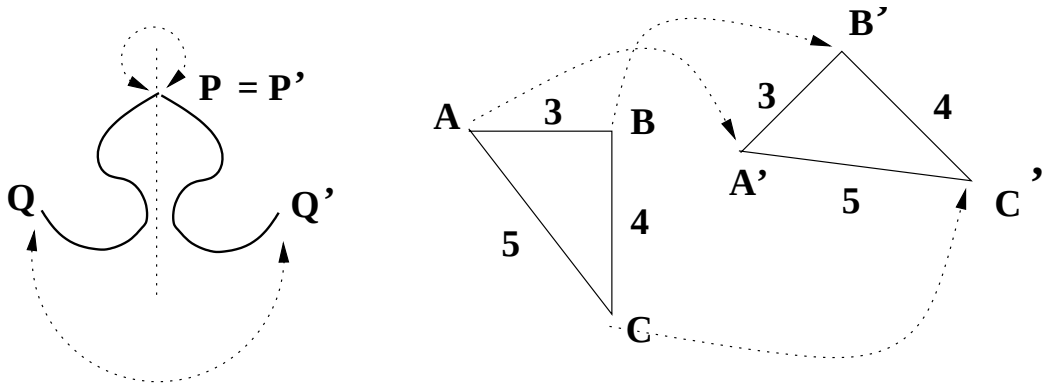
We let $\mathbb{E}$ denote (the set of points in) the *Euclidean plane*. In fact, many of our results will extend to Euclidean spaces of higher dimension.

So let us try to make mathematical sense of motions and symmetry.

1. Think about **motion** of a figure in the plane. Freeze a couple of positions.



Or consider **symmetry** or **congruence**:



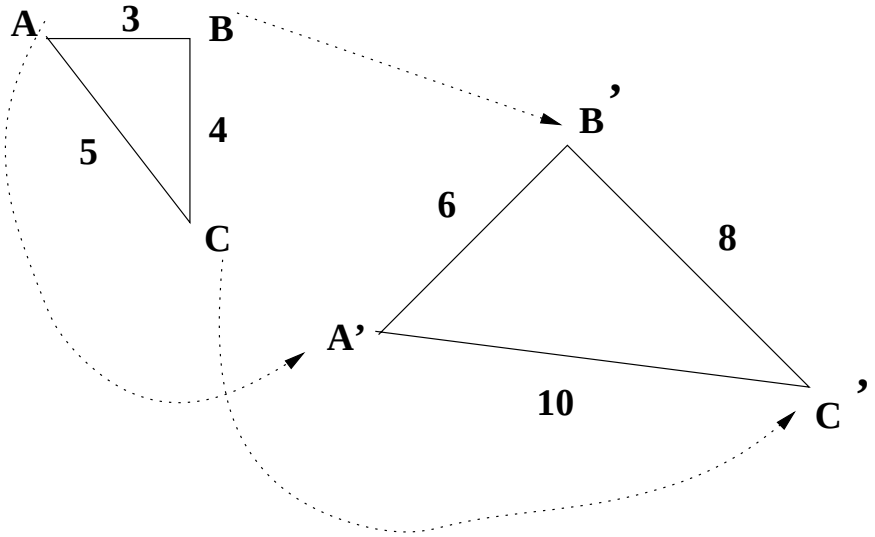
In all these examples, the geometrical operation gives a function f mapping P to P', A to A', etc. The function preserves shape; specifically, it preserves the distance between pairs of points in the figure:

$$PQ = P'Q'$$

for all points P, Q in the figure. Since the distance between constituent points is *invariant*, the shape as a whole is unchanged.

Every motion or symmetry can be reversed: just reverse the arrows and map P to P', etc. We get the function f^{-1}.

The idea of **similarity** is much like this, except that every distance now is rescaled by a constant positive factor.



2. What we have then are certain nice functions mapping a subset of $\mathbb{E}$ to another (possibly the same) subset of $\mathbb{E}$. It is convenient to simply take functions mapping all of $\mathbb{E}$ to $\mathbb{E}$, since we can then simply restrict our attention to any particular subset of interest.

   For example, a symmetry of the square is really descended from an isometry of the whole plane; but we usually ignore what that isometry does outside the square.

3. Such functions must have some very basic properties to preserve the integrity of the plane. We cannot collapes two points to one: f must be $1-1$ (or *injective*). And f must not leave any point of the plane missing after the fact: it must be onto (or *surjective*).

   In short, we consider *bijections*

   $$f : \mathbb{E} \to \mathbb{E},$$

   typically with some nice property. For example, an *isometry* of $\mathbb{E}$ is any bijection which preserves all distances.

   Any such bijection has an inverse

   $$f^{-1} : \mathbb{E} \to \mathbb{E}$$

   defined by $f^{-1}(A) = B$ whenever $f(B) = A$, for points $A, B \in \mathbb{E}$. In effect, you just reverse the arrows in the above pictures.

   Any bijection defines a $1-1$ correspondence between the points of its domain and the points of its range. These sets therefore have exactly the same *cardinality*, whether infinite or not.

   In our considerations, the domain and range will usually be the same set $\mathbb{E}$.

4. The bijections from X to Y have properties which remind us of the group axioms. However, we do need an identity and this forces $X = Y$.

   Definition Let X be any non-empty set, finite or infinite. Let

   $$\mathbb{S}_X = \{\text{all bijections } f : X \to X\},$$

   equipped with composition $f \circ g$ as operation.

   (a) Verify that $f \circ g$ is a binary operation on $\mathbb{S}_X$.

   (b) Verify that $\mathbb{S}_X$ is a group. (Mostly this was done in earlier exercises.)

   Thus we have lots of groups of a particular kind: $\mathbb{S}_X$ is called the symmetric group on set X.

   Exercises on Symmetric Groups

   (a) If X is finite, say with n elements, how many bijections $f : X \to X$ are there? (Think: given n people in n chairs, how many ways can they rearrange themselves?)

   (b) If $|X| = n$ (meaning "X has n elements") then $\mathbb{S}_X$ has what order?

   (c) Could $\mathbb{S}_X$ ever be a commutative group?

6 Subsets and subgroups

Here G is any group, finite or infinite, with the operation written as multiplication. So ab could mean $a \times b$, $a + b$, etc.

1. (a) Suppose A, B are non-empty subsets of G. Then we define

$$AB := \{ab : \ a \in A \ \text{ and } \ b \in B\}.$$

In short, take all possible products, first an element of A, then an element of B.

(b) A or B could have one element $g \in G$. Then we usually write

$$Ag \text{ (instead of } A\{g\})$$
$$gB \text{ (instead of } \{g\}B).$$

(c) Similarly, we define

$$A^{-1} := \{a^{-1} : \ a \in A\}.$$

(d) **Exercises**. Suppose A, B, C are subsets of G.

1.1 Show $(AB)C = A(BC)$ and $(A^{-1})^{-1} = A$.

1.2 Show that A, Ag, gA have the same size.

1.3 Give an example of subsets A, B of S_3 with $|A| = 3$, $|B| = 2$ but $|AB| \neq 6$.

1.4 Rewrite the objects in exercises 1.1 and 1.2 in *additive notation*.

1.5 Show that $GG = G$.

2. **SUBGROUPS**

(a) A subset H of G is a *subgroup* if it is a group in its own right, with the operation inherited from G.

Note that associativity is inherited for any subset. Thus for H to be a subgroup we really mean:

(i) $1 \in H$.

(ii) $a, b \in H \Longrightarrow ab \in H$
(i.e. elements in H also have their product in H, in short the group operation is closed on H).

(iii) $b \in H \Longrightarrow b^{-1} \in H$
(i.e. elements in H have inverses also in H – inverting is also closed on H).

(b) **Exercises**.

2.1 **Subgroup Test**. A non-empty subset H of G is a subgroup if and only if

$$a, b \in H \Longrightarrow ab^{-1} \in H.$$

2.2 H is a subgroup if and only if $HH^{-1} \subseteq H$.

2.3 If H is a subgroup, then $H = H^{-1}$ and $HH = H$.

2.4 **Example**: Let

$$\begin{aligned} G &= \{2^k : k \in Z\} \\ &= \{\ldots \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4 \ldots\} \end{aligned}$$

with ordinary multiplication.

Exercises:

2.41 Show that G is a group. Thus G is a subgroup of the positive reals, with ordinary multiplication.

2.42 Convince yourself that G is isomorphic to $(Z, +)$. In particular, G is abelian.

2.43 Find a subset $H \subset G$ such that $HH = H$ but H is <u>not</u> a subgroup.

2.5 (Compare 2.43 above). Suppose H is a finite subset of any group G, and

$$HH = H.$$

Show that H <u>is</u> a subgroup.

(c) **Definition** If $a \in G$, then the *cyclic* subgroup generated by a is

$$\langle a \rangle := \{a^k : k \in Z\} .$$

(Consider example 2.4 above).

(d) **More Exercises**.

2.6 Show that $\langle a \rangle$ actually is a subgroup and is, furthermore, abelian.

2.7 Give examples of G and $a \in G$ in which $\langle a \rangle$ is infinite. Likewise finite.

Definition. The *order* of any $a \in G$ can be defined as the smallest positive integer n (if any exists) for which $a^n = 1$. We write

$$|a| = n.$$

If no such n exists, we say a has infinite order: $|a| = \infty$.

2.8 <u>Exercise</u>. Show that $|a| = |\langle a \rangle|$. (The order of a also equals the number of elements in the subgroup generated by a).

3. COSETS

When a subset H of G is actually a subgroup, the sets Hg are particularly nicely behaved. For any $g \in G$, we say:

Hg is a *right coset* of H
gH is a *left coset* of H.

Right and left cosets have analogous properties. So for now let's look only at right cosets.

(a) We have already seen that, for any $g \in G$,

$$|gH| = |H| = |Hg|.$$

That is, all cosets have the same size, namely the size of H.
Indeed, any subgroup H is itself a coset (of itself):

$$H = H1.$$

(b) **Exercise** 3.1. Let S_3 be the group of all permutations on three things, say $\{1, 2, 3\}$. We call S_3 the symmetric group of degree 3. Its order is $3! = 6$, and

$$S_3 = \{(1), (123), (132), (12), (13), (23)\}.$$

Let $H = \langle (12) \rangle = \{(1), (12)\}$ (a cyclic subgroup).
Find − all right cosets of H.
− a set of right coset representatives (namely, pick an individual element from each coset).
− all left cosets of H.
Are the left and right cosets identical?

Exercise 3.2. Try to make *Gap* find all right cosets of H in S_3 (from Exercise 3.1). Try to make *Gap* find a set of right coset representatives.

(c) **Theorem**: (i) $Ha = Hb$ if and only if $ab^{-1} \in H$.
(ii) $aH = bH$ if and only if $b^{-1}a \in H$.

Proof. Part (ii) is similar to part (i). In part (i), there are two things to show.

Assume	$Ha = Hb$.	Since $1 \in H$
	$1a = hb$,	for some $h \in H$.
Thus	$ab^{-1} = h \in H$.	
Assume	$ab^{-1} \in H$. We must show $Ha = Hb$.	
Suppose	$x \in Ha$, say $x = ha$. Then	
	$xb^{-1} = h(ab^{-1}) = hh'$, where $h' \in H$.	
So	$xb^{-1} = \tilde{h} \in H$	
so	$x = \tilde{h}b \in Hb$.	
Thus	$Ha \subseteq Hb$.	
Similarly	$Hb \subseteq Ha$: we're done.	

(d) **Coset Representatives**
If Ha is any coset, then "a" is called a coset representative for the coset Ha. There can be many coset representatives, since $Ha = Hb$ if $ab^{-1} \in H$. Thus, if "a" is one representative, then any $ha = b$ is another ($h \in H$).
In particular, $H = Hb$ whenever $b \in H$.

(e) **Theorem**. Any two right cosets are either identical or disjoint. (The same is true for two left cosets.)

Proof. Let Ha and Hb be two cosets of the subgroup H.
If they are disjoint (meaning no elements in common) we are done:

$$Ha \cap Hb = \emptyset.$$

So suppose Ha and Hb have at least one element in common, say

$$x \in Ha \cap Hb.$$

The point is that this forces the cosets to be completely the same. Indeed,

$$x \in Ha, \text{ so } x = h_1 a \text{ where } h_1 \in H$$
$$\text{and } x \in Hb, \text{ so } x = h_2 b \text{ where } h_2 \in H.$$

So $$a = h_1^{-1}x, \;\; b = h_2^{-1}x, \;\; b^{-1} = x^{-1}h_2,$$

and thus:

$$\begin{aligned} ab^{-1} &= (h_1^{-1}x)(x^{-1}h_2) \\ &= h_1^{-1}h_2 \in H. \end{aligned}$$

By the Theorem 3(c), $Ha = Hb$.

(f) **Theorem**. Every element of G belongs to exactly one coset of H.
Proof. Say $g \in G$. Then $g = 1g$, so $g \in Hg$. By Theorem 3(e), g cannot belong to two *different* cosets. Yes, maybe $Hg = Ha$, but that is the *same* coset. □

Suppose now that there are finitely many cosets of the subgroup H in G. This happens when G itself is finite, but also in other cases.
We may represent the k cosets by

$$1 = a_0, a_1, a_2, \ldots, a_{k-1},$$

so that the different cosets are $H = H1, \;\; Ha_1, \;\; Ha_2, \;\; \ldots, \;\; Ha_{k-1}$.
By Theorem 3(f), we can represent the situation diagrammatically like this:

G					
	H $= H1$	Ha_1	Ha_2	$\ldots$	Ha_{k-1}

But <u>all</u> cosets Ha_j have the same size, namely $|H|$.
So

$$\begin{aligned} |G| &= |H| + |H| + \ldots + |H| \\ &= k|H|. \end{aligned}$$

We have therefore proved an expected and important result:
Lagranges Theorem: If H is a subgroup of a finite group G, then $|H|$ divides $|G|$, and the *index*

$$[G : H] := \frac{|G|}{|H|}$$

is the number of right cosets of H. (Also, it is the number of left cosets.)

(g) Recall that any element $a \in G$ generates a cyclic group $\langle a \rangle$. We defined the order of a to be the smallest positive integer n such that

$$a^n = 1.$$

(And you should prove that this order equals the size of the corresponding cyclic subgroup.)

Exercise 3.2. Suppose that G is finite and $a \in G$. Then $|a|$ divides $|G|$.

Exercise 3.3. Suppose that $|G| = p$, a prime. Then G is a cyclic group.

Up to isomorphism, there is only one group of prime order p. It is cyclic, hence abelian.

Exercise 3.4. Let $G = \mathbb{R}^2$, with addition. So

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2,\ y_1 + y_2).$$

(.1) Show that G is an abelian group. What is the (unique) identity element? Of course, G is very infinite.

(.2) Let $H = \{(x, 2x) :\ x \in \mathbb{R}\}$. Show that H is a subgroup of G. Describe H and its right cosets geometrically. In light of this interpret 3(c), 3(e), 3(f).

(h) **Exercise 3.5**. Suppose G is a finite group and H, K are subgroups with $K \subseteq H \subseteq G$.

Show: $[G : K] = [G : H] \cdot [H : K]$.

Note:

$$\text{index is } [G : K] \left\{ \begin{array}{ll} G & \\ | & \text{index is the integer} [G : H] \\ H & \\ | & \text{index is the integer} [H : K] \\ K & \end{array} \right.$$

(i) **Exercise 3.6**. Let G be any group, perhaps infinite.

(i) Suppose H_1 and H_2 are subgroups. Show that $H_1 \cap H_2$ is also a subgroup.

(ii) More generally, suppose $\{H_t : t \in \mathcal{I}\}$ is any collection of subgroups. (That is, the index set can be finite or not; the individual groups can be finite or not.) Show that

$$H = \bigcap_{t \in \mathcal{I}} H_t$$

is a subgroup of G.

4. Let X be any subset of the group G. X need not be a subgroup. By a *word* in X we mean any product.

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k}$$

where $\varepsilon_j = \pm 1$ and each $x_j \in X$. For example,

$$1 = x_1^1 \cdot x_1^{-1}$$
$$x_1^3 = x_1^1 x_1^1 x_1^1$$
$$x_1 x_2^{-1} x_1 x_3 x_4^{-1}$$

are words in $X = \{x_1, x_2, x_3, x_4\}$.

The subgroup *generated* by X is the set of all words in X. We write

$$\langle X \rangle = \{\text{words } x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k} \text{ in } X\}.$$

(a) **Exercise 4.1**. Verify that $\langle X \rangle$ is indeed a subgroup. Hint: Use exercise 2.1.

(b) **Exercise 4.2**. Show that $\langle X \rangle$ is the intersection of all subgroups of G which contain X. (There is at least one such subgroup, namely G itself.)

Remark: this provides an alternative definition for the subgroup generated by a subset X of the group G.

Intuitively, we may therefore say that $\langle X \rangle$ is the *smallest* subgroup which contains the set X.

5. **Normal Subgroups**

Again H is some subgroup of G, perhaps finite or not.

(a) We look at right cosets, though Theorem 6(e) below shows that we could just as well use left cosets.

(b) Now $H = H1$ is itself a coset, and

$$HH = H.$$

In fact, for any coset Hb $\quad (b \in G)$ we have

$$H(Hb) = (HH)b = Hb.$$

Thus H acts like an identity for multiplication of cosets.

(c) Someone's wonderful idea was to try to make a new group, denoted

$$G/H$$

with:

(i) the cosets $Hb \quad (b \in G)$ as individual elements.

(ii) coset multiplication as operation.

(iii) the coset H itself as identity.

(d) The key difficulty in verifying that this even makes sense is that for certain subgroups H, multiplication of cosets need not be a closed operation.

Exercise 5.1. $G = S_3$ (order 6)
$H = \langle (12) \rangle$ (order 2)
$a = (23) \qquad b = (13)$

Find $Ha, \ Hb$ then show that $HaHb$ is not even a coset.

(e) Thus we have good reason to study subgroups H for which coset multiplication is closed.

Definition. H is a *normal* subgroup of G, written

$$H \lhd G,$$

if coset multiplication is closed.

There are many useful and equivalent ways to say the same thing. Some of these equivalent ways are given in the next theorem.

It will be useful now to recall that

$$x \in Hg \text{ if and only if } Hg = Hx.$$

6. **Theorem** (*Criteria for Normality*)

The following items are equivalent for a subgroup H of G.

(a) H is normal in G [meaning "coset multiplication is closed"].

(b) $(Ha)(Hb) = Hab \qquad$ for all $a, b \in G$.

(c) $a^{-1}Ha \subseteq H \qquad$ for all $a \in G$.

(d) $a^{-1}Ha = H \qquad$ for all $a \in G$.

(e) $Ha = aH \qquad$ for all $a \in G$.
Caution! This need not mean that a commutes with all *individual* elements of H.

(f) Every right coset of H equals some left coset.

Proof. We must show that each of the six conditions implies each of the five others, for a tentative total of 30 separate proofs!! However, we get the same result much more economically by showing

$$(a) \Rightarrow (b), (b) \Rightarrow (c), (c) \Rightarrow (d), (d) \Rightarrow (e), (e) \Rightarrow (f) \text{ and } (f) \Rightarrow (a).$$

Here are the details.

$(a) \Rightarrow (b)$ Assume $Ha,\ \ Hb$ are any cosets, so that

$$(Ha)(Hb) = Hg \qquad \text{for some unknown } g \in G.$$
$$\text{But then } (1a)(1b) = ab \in Hg, \text{ so}$$
$$Hg = Hab$$
$$\text{Thus } (Ha)(Hb) = Hab.$$

$(b) \Rightarrow (c)$ For any $a \in G$,

$$Ha^{-1}Ha = H(a^{-1}a) = H1 = H.$$
$$\text{Now let } x \in a^{-1}Ha. \text{ Then } x = a^{-1}ha, \text{ for some } h \in H.$$
$$\text{Thus } x = 1a^{-1}ha \in Ha^{-1}Ha = H.$$
$$\text{So } x \in H.$$

Since x was arbitrary in $a^{-1}Ha$, we get

$$a^{-1}Ha \subseteq H.$$

$(c) \Rightarrow (d)$ For any $a \in G$, $\quad a^{-1}Ha \subseteq H$. In particular, this is also true when a is replaced by a^{-1}:

$$(a^{-1})^{-1}H(a^{-1}) \subseteq H$$
$$aHa^{-1} \subseteq H$$
$$\text{so } a^{-1}(aHa^{-1})a \subseteq a^{-1}Ha$$
$$\text{so } 1H1 \subseteq a^{-1}Ha$$
$$\text{so } H \subseteq a^{-1}Ha \subseteq H$$
$$\text{Thus } a^{-1}Ha = H.$$

$(d) \Rightarrow (e)$ If $a^{-1}Ha = H$, then

$$a(a^{-1}Ha) = aH$$
$$1Ha = aH$$
$$Ha = aH$$

$(e) \Rightarrow (f)$ Every right coset $Ha = aH$, a left coset.

$(f) \Rightarrow (a)$ Assume every right coset equals some left coset and consider any $a, b \in G$. We want to multiply two right cosets Ha and Hb. But the left coset aH is some right coset, say

$$* \quad aH = Hc, \qquad \text{for some unknown } c.$$

Thus

$$\begin{aligned}(Ha)(Hb) &= H(aH)b \\ &= H(Hc)b \\ &= (HH)(cb) \\ &= H(cb),\end{aligned}$$

so that right coset multiplication is closed.

Remark: Since $a \in aH = Hc$, we could have chosen $c = a$, obtaining $aH = Ha$, then

$$(Ha)(Hb) = H(ab).$$

This finishes the proof. □

7. **The Factor Theorem**

Suppose $H \lhd G$ (H is a normal subgroup of G). Then

$$G/H \quad \text{(the family of right cosets of } H)$$

forms a group with coset multiplication. The identity is H, and Ha has inverse $H(a^{-1})$.

Proof. We know the operation is closed. It's easy to check associativity, the identity and inverses. □

Remark. (i) G/H is called a *quotient* group, or sometimes a *factor group*.

(ii) By Theorem 6(e), we could just as well use left cosets.

8. **Exercises**

(a) **Exercise 8.1**. $G \lhd G$ and $\{1\} \lhd G$. Thus, the trivial subgroups of G are each normal.

(b) **Exercise 8.2**. If G is abelian, then every subgroup is normal.

(c) **Exercise 8.3**. If $[G : H] = 2$, then $H \lhd G$.

(d) **Exercise 8.4**. If $H \lhd G$ and $[G : H] = k$, then

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

(e) Generally a group G has lots of subgroups, say the cyclic subgroups generated by one element a, and also subgroups generated by two or more elements.

Also, by Exercise 8.2, every subgroup of an abelian group is normal. However, for non-abelian groups G it sometimes happens that normal subgroups are scarce. Such groups G are interesting and important: we call them simple.

Definition. A group G is *simple* if it has *no* non-trivial normal subgroups. (Thus, $\{1\}$ and G are the only normal subgroups.)

Remark: in a sense, simple groups play the same role in group theory as prime numbers play in number theory. The actual details in either case are very deep and complicated.

(f) **Exercise 8.5**. Characterize all cyclic groups which are simple. (Hint: $\langle a \rangle$ of order n or order ∞ is abelian: use Exercise 8.2.)

(g) **Exercise 8.6**. If $\{H_t : t \in \mathcal{I}\}$ is any family of normal subgroups of G, then

$$H = \bigcap_{t \in \mathcal{I}} H_t$$

is also a normal subgroup.

Remark. In particular, if H_1 and H_2 are normal, so is $H_1 \cap H_2$.

(h) **Definition**. If $x, b \in G$, then $x^{-1}bx$ is called a *conjugate* of b. If S is any subset of G, let

$$\tilde{S} = \{x^{-1}sx \ : \ s \in S, \ \ x \in G\}$$

be the set of all conjugates of elements of S.

(i) **Exercise 8.7**. Show that $H = \langle \tilde{S} \rangle$ is a normal subgroup of G and that $H \subseteq S$.

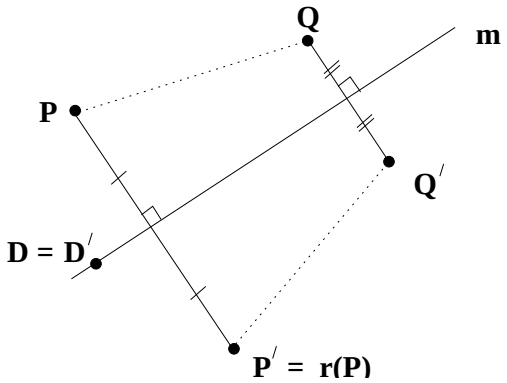
Show that H is the intersection of all normal subgroups of G which contain S. (In some sense, H is the *smallest* normal subgroup containing S.)

Definition. $H = \langle \tilde{S} \rangle$ is the *normal closure* of G.

7 Some useful mappings on the plane $\mathbb{E}$.

1. **The reflection r in a given line m**

   Definition For each point P let $r(P)$ be the point on the line through P and perpendicular to m, but an equal distance from m on the opposite side:



   (a) r is well-defined (that is, there can't be two such perpendiculars; but consider the north pole and equator on the sphere; something subtle is going on!). This is a purely geometric definition, valid in the non-Euclidean plane, too. In particular, we need not use coordinates as part of the definition.

   (b) For each point $P \in \mathbb{E}$

   $$r(r(P)) = P\,,$$

   that is,

   $$r \circ r = 1$$

   where $1 = 1_{\mathbb{E}}$ is the identity mapping on $\mathbb{E}$. Briefly we write $r^2 = 1$. This algebraic condition actually implies that r is a bijection; and we have $r = r^{-1}$. A mapping like r which has period 2 is called an *involution*.

   (c) A point D is *fixed* or *invariant* if $r(D) = D$. For a reflection r this occurs if and only if $D \in m$.

   (d) r preserves distance. For ease of notation let

   $$\begin{aligned} P' &= r(P) \\ Q' &= r(Q). \end{aligned}$$

   Using a few applications of SAS we conclude that $PQ = P'Q'$ in the above diagram, regardless of the location of points P and Q relative to m. (Exercise: do the case in which P and Q lie on opposite sides of m.) Thus r is an isometry:

   (e) **Definition:** An *isometry* (of the plane $\mathbb{E}$) is a distance preserving bijection $f : \mathbb{E} \to \mathbb{E}$.

   Intuitively isometries preserve shape because of this. In this regard, it is useful to note the following

(f) **Lemma:** The collection of all points X equidistant from two distinct points P, Q is a line (the *perpendicular bisector* of segment PQ).

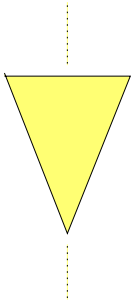
Proof. Uses only a few applications of basic congruence theorems, such as SAS. □

(g) Thus any isometry (in particular any reflection)

- maps a circle to a (congruent) circle of the same radius
- maps a straight line to a straight line
- maps a triangle $\triangle ABC$ to a congruent $\triangle A'B'C'$

(h) A reflection r is *opposite*: see the above figure. P, Q, D form a clockwise cycle, whereas their images P', Q', D' form an anticlockwise cycle.

(i) r is defined on all of $\mathbb{E}$; in typical applications we restrict to a subset of interest

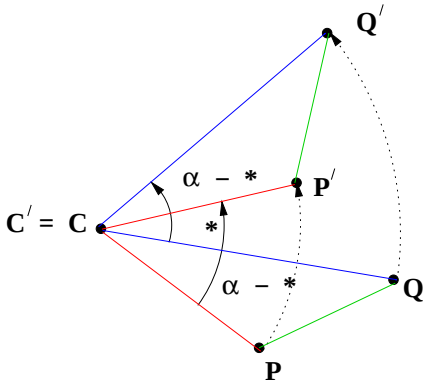


Here the subset is an isosceles triangle, which has bilateral symmetry.

2. **The rotation s with centre C and angle α**

Definition. For each point $P \in \mathbb{E}$ let $P' = s(P)$ be the same distance from C as P and located so that

$$\measuredangle PCP' = \alpha.$$



(a) Again it is easy to check that this description is well-defined and that s is a bijection. Once more an application of SAS shows that s is an isometry. You can see from the figure that $\triangle PQC$ and $\triangle P'Q'C'$ have the same *orientation*. (Note that the centre $C = C'$ is invariant.) Thus a rotation s is a *direct* isometry.

(b) Note that we must distinguish clockwise from anticlockwise rotations. We do this in the usual manner, taking

$$\alpha : \begin{array}{l} \oplus \text{ if anti-clockwise} \\ \ominus \text{ if clockwise} \end{array} .$$

(c) If $\widehat{s}$ is the rotation with the same centre C, but with the opposite angle $-\alpha$, then $s(P) = P'$ implies $\widehat{s}(P') = P$. Thus

$$s \circ \widehat{s} = 1 = \widehat{s} \circ s.$$

Therefore the inverse of a rotation s is also a rotation; and s^{-1} has the same centre as s, but the opposite angle.

(d) If $\alpha = 0°,\ \pm 360°,\ n(360°)$ and C is any centre, then

$$s = 1 .$$

Thus the identity is actually a rotation with ambiguous centre.

Otherwise, if $\alpha \neq n(360°)$, where $n \in \mathbb{Z}$, then s fixes only C.

(e) In any rotation, the angles $\alpha + n(360°)$ all define the same rotation, here considered to be a fixed mapping on the plane.

(f) **Definition:** The *half-turn* $h = h_C$ with centre C is the rotation at C with angle 180°.

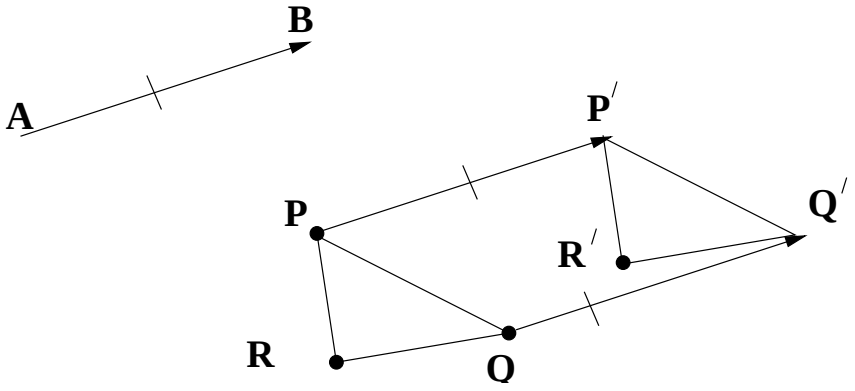
Observe that every half-turn is an involution.

3. There could be other kinds of isometry. So far, we have two distinct species. In fact, it will follow from the three reflections theorem and the nature of Euclidean parallelism, that there are just two more species of Euclidean isometries: *translations* and *glides*.

4. **The translation t with vector $\vec{AB}$**

Recall that vector $\vec{AB}$ is the directed line segment from point A (the tail) to point B (the head).

Definition The **translation** t with vector $\vec{AB}$ maps point $P \in \mathbb{E}$ to the point $P' = t(P)$ located so that $\overrightarrow{AB}$, $\overrightarrow{PP'}$ are equal and parallel, in the same sense. (We say that these two vectors are equal, of course.)



(a) You may check that t is an isometry. The verification uses properties of parallel lines and hence is heavily dependent on Euclidean parallelism.

(b) t is direct: triangles PQR and $P'Q'R'$ have the same orientation.

(c) The inverse of translation t is another translation; and t^{-1} has vector $\vec{BA} = -\vec{AB}$.

(d) The identity 1 can be considered anew as a translation with the vector $\vec{0} = \vec{AA}$.

5. **The glide (or glide reflection) g with non-zero axial vector $\vec{AB}$**

Definition The **glide** g with *axial vector* $\vec{AB}$ is the product of the translation t with vector $\vec{AB}$ and the reflection r in the line through A and B. (We insist that $\vec{AB} \neq \vec{0}$ merely to guarantee that A, B are distinct points.) Thus

$$g = rt\ .$$

(a) In this set up we actually have $rt = tr$. Prove this! Thus the definition is not as touchy as one might think.

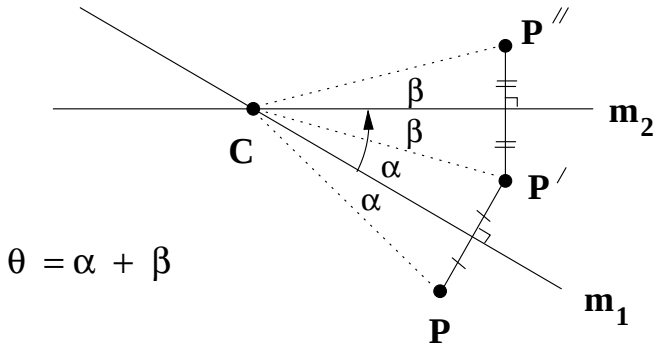
(b) The line through A and B is callled the *axis* of the glide.

(c) Since we have defined a glide as a product of two isometries, it must itself be an isometry. In fact, g^{-1} is a also a glide, with the opposite axial vector $\vec{BA} = -\vec{AB}$, The actual axis is the same.

(d) Being a product of a direct and opposite isometry, a glide must itself be opposite.

8 Practical calculations with isometries.

1. **Theorem** Suppose lines m_1, m_2 meet at C and the angle *from* m_1 *to* m_2 is θ:



Let r_j be the reflection with mirror m_j. Then $r_2 r_1$ is the rotation with centre C and angle 2θ.

Proof. See the diagram. Note that this result does not depend on explicit properties of parallelism. It holds in non-Euclidean geometry, too. □

(a) Note the interaction of species here. A analogous result holds when m_1 and m_2 are parallel. In that case $r_2 r_1$ is the translation through *twice* the vector running orthogonally from m_1 to m_2.

(b) How is θ ambiguous? Why doesn't it matter?

(c) Order does matter. Usually $r_1 r_2 \neq r_2 r_1$.

(d) If $m_1 = m_2$, then $r_1 = r_2$ and $r_2 r_1 = r_1 r_1 = 1$. Suppose $m_1 \neq m_2$. When does $r_1 r_2 = r_2 r_1$?
Answer: When $m_1 \perp m_2$ and then $r_1 r_2 = r_2 r_1 = h_C$.

(e) $r_2 r_1 = s =$ rotation with centre C, and angle 2θ.

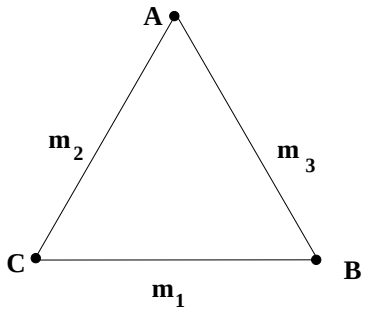
$\uparrow\uparrow$	$\uparrow$
mirrors m_1, m_2 through C	no mirrors any more!

The devious insight here comes from turning this around. Given a rotation s we can factor

$$s = r_2 r_1$$

choosing m_1 (or m_2) through C arbitrarily, adjusting m_2 (or m_1) appropriately.

2. Example.



(a) let r_j be reflection in m_j. Compute r_2r_1, r_1r_2, $r_1r_2r_1$ and $r_2r_1r_2$.

(b) Let $s = 60°$ rotation at C and $\tilde{s} = 60°$ rotation at B. Compute $s\tilde{s}$, $\tilde{s}s$ and $s\tilde{s}^{-1}$.

9 Subgroups of the group of all isometries

1. The collection of all isometries f of $\mathbb{E}$ forms an infinite group *ISOM*.
   Verify this.

2. Interesting subgroups of *ISOM*.
   Definition. By a figure K in the plane we mean any subset $K \subseteq \mathbb{E}$.

   (a) The *symmetry group* of K is

   $$\text{Sym}(K) = \{ \text{ isometries } f \text{ which map } K \text{ onto itself (globally)}\}$$

   Note that although $f(K) = K$ for all $f \in \text{Sym}(K)$, it is quite possible for the constituent points $P \in K$ to move 'internally'.
   Why is a Sym(K) a group?

   (b) In more restricted fashion, we define Fix(K) to be the collection of all isometries which fix each point of K.
   Verify that Fix(K) is indeed a group.

   (c) In fact we have these subgroup relationships:

   $$\text{Fix } (K) \subseteq \text{ Sym } (K) \subseteq \text{ Isom.}$$

3. Examples. Clearly describe all isometries in Fix (K) and Sym (K) when

   (a) $K = \{A, B\}$ (two distinct points).

   (b) K is a line m.

   (c) K is a circle.

   (d) $K = \emptyset$ (the empty set).

(e) $K = \{O\}$, one specific point. In this case Fix (O) = Sym (O) ! The resulting infinite group is called the *orthogonal group* for the plane. We sometimes denote it by $O(\mathbb{E})$.

Convince yourself that the orthogonal group at O consists of all rotations with centre O (including 1), together with all reflections in lines through O.

The rotations alone constitute a subgroup of index 2 in $O(\mathbb{E})$; this subgroup is called the *special orthogonal group* and is denoted $SO(\mathbb{E})$.

4. **Note**: Rather similar things happen in $n \geqslant 3$ dimensions, though the details are somewhat more intricate. For example, in Euclidean 3-space there are 6 species of isometry.

10 Justifying our Intuition.

1. If ABC is any triangle in $\mathbb{E}$, then each point $P \in \mathbb{E}$ is uniquely determined by its distances (in order) to A, B, C.

   Proof. Use the Lemma on the perpendicular bisector. □

2. The action of an isometry f on any specific triangle.

   Suppose

   $$f : ABC \to A'B'C'.$$

   Then

   $$\triangle ABC \equiv \triangle A'B'C'.$$

   Proof. Use SSS. □

3. Suppose ABC are the vertices of a triangle. If $f : ABC \to ABC$, then $f = 1$.

   (We mean of course that f maps the vertices in order; thus f fixes each vertex of $\triangle ABC$.)

   Proof. Again use the Lemma on the perpendicular bisector. □

4. If both $f, g = ABC \to A'B'C'$, then $f = g$.

   Proof. Use the previous result! □

   Meaning: Each isometry is completely determined by its effect on one particular triangle. There may be a convenient triangle which makes the calculations easy.

5. **Exercise**. Reprove the theorem that a product of reflections in intersecting mirrors is a particular rotation. Ditto when the mirrors are parallel.

6. **The Three Reflections Theorem** Any isometry $f : \mathbb{E} \to \mathbb{E}$ is a product of at most three reflections.

   Remark: This is an absolute theorem. It holds just as well in the non-Euclidean plane $\mathbb{H}^2$. However, the details for the various species there play out in a slightly different way. Indeed in $\mathbb{H}^2$ there are 5 rather than 4 species.

   Proof. Pick any one triangle $\triangle ABC$ to work with. Suppose $f : ABC \to A'B'C'$, so that $AB = A'B'$, $AC = A'C'$ and $BC = B'C'$.

   (a) If necessary, i.e. if $A \neq A'$, apply to $\triangle ABC$ reflection r_1 in the perpendicular bisector of segment AA'. Thus r_1 maps $\triangle ABC$ to the congruent triangle $\triangle A'B''C''$. Thus $A'B' = AB = A'B''$, so that A' is on the perpendicular bisector of segment $B'B''$.

   (b) If necessary, i.e. if $B' \neq B''$, apply reflection r_2 in the perpendicular bisector of segment $B'B''$. Thus r_2 fixes A' and maps $\triangle A'B''C''$ to the congruent triangle $\triangle A'B'C'''$.

   (c) Now both A' and B' are on the perpendicular bisector of segment $C'C'''$. If necessary, i.e. if $C''' \neq C'$, apply reflection r_3 in the perpendicular bisector of segment $C'C'''$. Then r_3 maps $\triangle A'B'C'''$ to the congruent triangle $\triangle A'B'C'$.

   In summary, the product $r_3r_2r_1$ (with the unnecessary reflections deleted) maps $\triangle ABC$ to $\triangle A'B'C'$. Thus $f = r_3r_2r_1$. □

7. (a) **Corollary 1:** If f fixes a point O, at most 2 reflections are required. Thus every isometry fixing a point O is a rotation centred at O, or a reflection in some line through O.

   (This solves an earlier problem on the constitution of the orthogonal group $O(\mathbb{E})$.)

   (b) **Corollary 2:** If f fixes two points $A \neq B$, then either $f = 1$ or f is the reflection in the line AB.

   (c) **Remarks**: From these results, it is now a routine matter to classify all isometries in *ISOM*. Similarly, in Euclidean n-space, every isometry is the product of at most $n + 1$ reflections.

8. Let K be any subset of $\mathbb{E}$, infinite or not. In many cases of interest there are *finitely many points* $P_1, \ldots, P_n \in K$ which are permuted amongst themselves by all isometries $f \in \mathrm{Sym}(K)$. (Think of a square K whose vertices are P_1, P_2, P_3, P_4.) In short, we have

$$\mathrm{Sym}(K) \subseteq \mathrm{Sym}(\{P_1, \ldots, P_n\}) .$$

In such cases, we can define a function

$$\varphi : \mathrm{Sym}(K) \to \mathbb{S}_n$$

by

$$(\varphi f)(i) = j$$

for $f \in \mathrm{Sym}(K)$ and whenever

$$\begin{aligned} f(P_i) &= P_j \\ (\ &= P_{(\varphi f)(i)}), \end{aligned}$$

$1 \leqslant i, j \leqslant n$.

Briefly, we try to track isometries by their *action* on a key set of points.

Theorem φ is a homomorphism.

This is a routine check. If $P_1, \ldots, P_n$ *do not all lie on one line* , then φ is $1-1$, by (3) just above. Furthermore, $\mathrm{Sym}(K)$ can be then identified with a subgroup of $\mathbb{S}_n$, the symmetric group on n symbols. In particular, $\mathrm{Sym}(K)$ is finite.

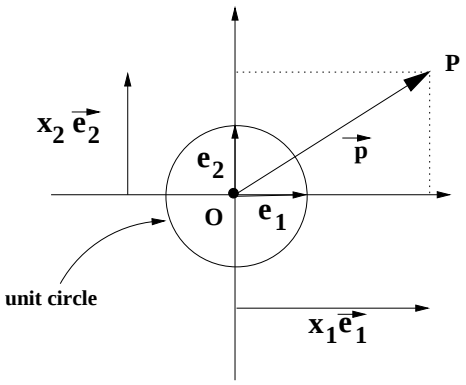
For example, the symmetry group of the square, which has order 8, is a subgroup of $\mathbb{S}_4$ (order 24).

11 Coordinates

Let O be any base point (origin). We thus know that the orthogonal group $O(\mathbb{E}) = \mathrm{Fix}(O)$ consists of all rotations centred at O together with all reflections in lines through O.

Project. Describe $O(\mathbb{E})$ algebraically using coordinates and matrices.

1. Having fixed an origin O, let's introduce the standard basis vectors $\vec{e_1}, \vec{e_2}$. These vectors are *orthonormal* : mutually perpendicular and each of length 1.



2. Any point $P \in \mathbb{E}$ can be located by its position vector $\vec{p} = \vec{OP}$. Since $\{\vec{e_1}, \vec{e_2}\}$ is a basis, *there exist unique* real numbers x_1, x_2 such that

$$\vec{p} = x_1\vec{e_1} + x_2\vec{e_2} \ .$$

Observe that (x_1, x_2) are the usual *rectangular coordinates* for P.

Remarks

(a) The fact that $\{\vec{e_1}, \vec{e_2}\}$ is a basis is equivalent to unique coordinates existing for each point $P \in \mathbb{E}$. This in turn is equivalent to having a *linearly independent spanning set* of vectors (here $\vec{e_1}, \vec{e_2}$).

(b) In the plane, any two vectors, neither of which is a multiple of the other, will serve as an alternate basis. Sometimes calculations are greatly simplified by working with a non-standard basis.

(c) For the purposes of calculations to come, it is very helpful to assemble the coordinates into a 2×1 column vector. Let us simply write

$$\vec{p} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \ .$$

It turns out that columns serve better than rows, since (illogically) we compose functions right to left.

(d) As examples, note that

$$\vec{e_1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \vec{e_2} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad \vec{o} = \vec{OO} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad .$$

(e) The geometrical linear combination

$$\vec{p} = x_1\vec{e_1} + x_2\vec{e_2}$$

becomes this component-wise calculation with column vectors:

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad .$$

(f) Having made these connections, we can now identify $\mathbb{E}$ with $\mathbb{R}^2$.

3. A *linear transformation* on $\mathbb{E}$ (well, on $\mathbb{R}^2$ to be precise) is a function which 'respects the vector' operations:

$$f : \mathbb{R}^2 \to \mathbb{R}^2$$

where

$$\begin{aligned} f(\vec{p} + \vec{q}) &= f(\vec{p}) + f(\vec{q}) \\ f(t\vec{p}) &= tf(\vec{p}) \end{aligned}$$

for all vectors $\vec{p}, \vec{q} \in \mathbb{R}^2$ and all scalars $t \in \mathbb{R}$.

Remarks:

(a) In general, f need not be $1-1$ or onto, although orthogonal isometries, being bijections, do have these properties.

(b) More generally, the domain and range could be different vector spaces, as in $f : V \to W$.

(c) Taking $t = 0$, we conclude that

$$f(\vec{0}) = \vec{0}$$

is forced.

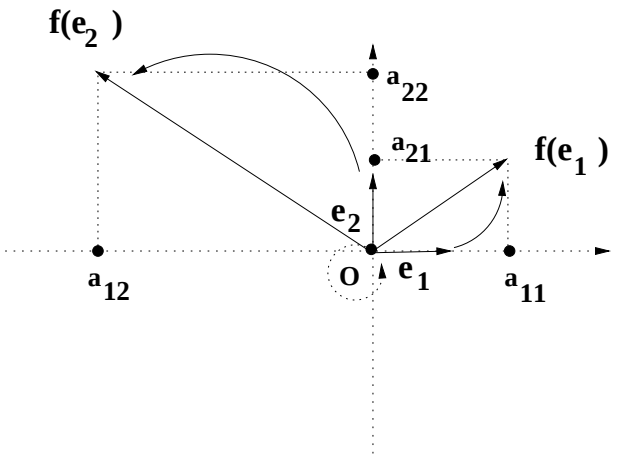
Now $f(\vec{e_1})$ and $f(\vec{e_2})$ are specific vectors. Suppose

$$f(\vec{e_1}) = f(\begin{bmatrix} 1 \\ 0 \end{bmatrix}) = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix}$$

and

$$f(\vec{e_2}) = f(\begin{bmatrix} 0 \\ 1 \end{bmatrix}) = \begin{bmatrix} a_{12} \\ a_{22} \end{bmatrix} \quad .$$

Thus in the scalar a_{ij}, the subscript i indicates the coordinate number, and the subscript j indicates the input number.



(The transformation f suggested in the figure definitely distorts distances and so could not represent an isometry.)

In general, if we apply f to

$$\vec{p} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} ,$$

we obtain

$$\begin{aligned} f(\vec{p}) &= f(x_1\vec{e_1} + x_2\vec{e_2}) \\ &= f(x_1\vec{e_1}) + f(x_2\vec{e_2}) \\ &= x_1 f(\vec{e_1}) + x_2 f(\vec{e_2}) \\ &= x_1 \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix} + x_2 \begin{bmatrix} a_{12} \\ a_{22} \end{bmatrix} \\ &= \begin{bmatrix} a_{11}x_1 + a_{12}x_2 \\ a_{21}x_1 + a_{22}x_2 \end{bmatrix} \\ &= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ &= A\vec{p} \ , \end{aligned}$$

where

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

is the fixed coefficient matrix for the linear transformation f. Note the natural roles of matrix addition, scalar multiplication and matrix multiplication.

4. In general, having chosen explicit bases, every linear transformation yields a matrix. The algebraic interaction of the linear transformations is exactly paralleled by the algebraic interaction of the matrices. (Technically, we have an *algebra isomorphism*.) For us, the key things to note are that

   (a) If f and g are linear transformations on $\mathbb{R}^2$, with 2×2 matrices A and B, respectively, then $f \circ g$, or just fg for simplicity, is also a linear transformation; and its matrix is the product AB.

   (b) The identity $1 = 1_{\mathbb{R}^2}$ is a linear transformation; and its matrix is the identity matrix
   $$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} .$$

   (c) If the linear transformation f is bijective, then the inverse function f^{-1} is also a linear transformation; and if f has matrix A, then f^{-1} has matrix A^{-1} (the matrix inverse).

   You should ponder and prove these claims.

   One conclusion to be made from these observations is that the collection of invertible linear transfromations from a vector space V to itself forms a group (as usual with compostion of functions for the operation).

   Definition: This group is denoted $GL(V)$. Likewise, the collection of all invertible 2×2 real matrices forms a non-abelian group, denoted
   $$GL_2(\mathbb{R}) .$$

5. **Keep in mind**: we could keep the same transformations, but change from the usual orthonormal basis $\{\vec{e_1}, \vec{e_2}\}$ to any other basis. The resulting matrices would very likely change, yet still describe the same geometric situation.

   Thus, we may guess that a wise, even unconventional, choice of basis may greatly simplify the matrix calculations.

6. We have strayed a bit from isometries into much more general territory. Let's return to isometries.

Theorem Any isometry f on $\mathbb{E}$, which fixes O, is an invertible linear transformation. With respect to the usual orthonormal basis $\{\vec{e_1}, \vec{e_2}\}$, each isometry f is represented by an *orthogonal* matrix A, namely a matrix satisfying

$$A^T A = I \ .$$

(Thus, very simply, $A^{-1} = A^T$.)

The orthogonal group $O(\mathbb{E})$, consisting of all isometries fixing an origin O, is isomorphic to the group $O_2(\mathbb{R})$ of all orthogonal 2 matrices. The direct isometries (rotations centred at O) correspond to orthogonal matrices with determinant $+1$. The opposite isometries (reflections in mirrors through O) correspond to orthogonal matrices with determinant -1.

Proof: The key is to remember that isometries preserve shapes, such as the shape of the parallelogram that underlies vector addition. Also an isometry preserves the ratios of lengths that underly scalar multiplication. One checks then that an isometry fixing O induces a linear transformation on $\mathbb{R}^2$.

In short, any isometry f is represented by some sort of 2×2 real matrix A. But what special property of A comes from f being an isometry?

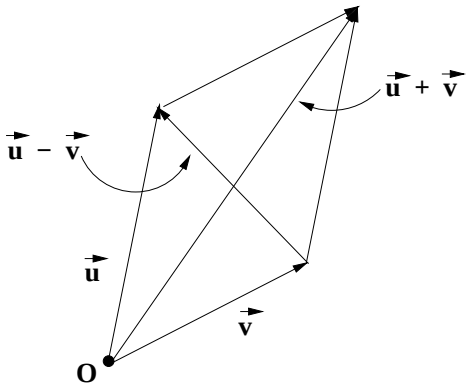
First, we note that f must preserve inner products To see this, suppose

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}, \vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \ .$$

Then

$$\begin{aligned} \vec{u} \cdot \vec{v} &= u_1 v_1 + u_2 v_2 \\ &= \frac{1}{4}[\ (u_1 + v_1)^2 + (u_2 + v_2)^2 - (u_1 - v_1)^2 - (u_2 - v_2)^2\ ] \\ &= \frac{1}{4}(\ \ \|\vec{u} + \vec{v}\|^2 - \|\vec{u} - \vec{v}\|^2\ \ ) \ . \end{aligned}$$

This *polarization identity* says that the inner product can be expressed in terms of the side and diagonal lengths in a suitable parallelogram:



Since any isometry f preserves the shape of this paralleogram, it must also preserve inner products:

$$f(\vec{u}) \cdot f(\vec{v}) = \vec{u} \cdot \vec{v}, \quad \forall \vec{u}, \vec{v} \in \mathbb{R}^2 \, .$$

But

$$\vec{u} \cdot \vec{v} = \vec{u}^T \vec{v} \, ,$$

where the 1×1 matrix product on the right is treated as a simple scalar. Hence, *for all* vectors $\vec{u}, \vec{v} \in \mathbb{R}^2$, we have

$$\begin{aligned} (A\vec{u})^T (A\vec{v}) &= \vec{u}^T \vec{v} \\ \vec{u}^T A^T A \vec{v} &= \vec{u}^T I \vec{v} \end{aligned}$$

where I is the 2×2 identity matrix. Since $\vec{u}, \vec{v}$ are arbitrary, we conclude that $A^T A = I$. □

7. **Exercises**

   (a) Give orthogonal matrices which describe

   - reflection in the x-axis
   - reflection in the y-axis
   - the half-turn h_O centred at the origin
   - the identity 1

   (b) Rotation matrices.

   - Give the *rotation matrix* A_α for the rotation s_α centred at O, through angle α.
   - What is A_0 ?
   - What is $A_{-\alpha}$?
   - Describe – on geometrical grounds – the product of isometries $s_\alpha s_\beta$.
   - Use the previous part to rewrite

     $$A_\alpha A_\beta$$

     as a single rotation matrix.
   - Look at the entries in theresulting matrix identity. What important facts have you proved?

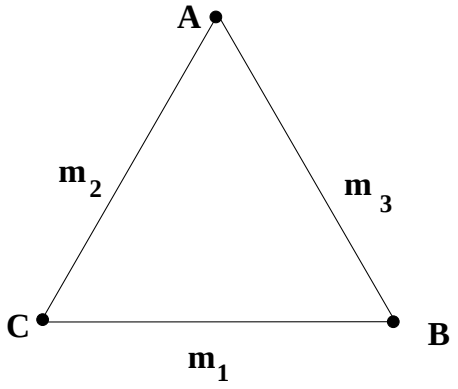
12 One Group from Several Points of View — Abstraction

1. **Geometrical Symmetry**: let G be the group of symmetries for an equilateral triangle. We know that there are three rotations, including the identity, say $1, s_1, s_2$, together with three reflections r_1, r_2, r_3. Thus

$$G = \{1, s_1, s_2, r_1, r_2, r_3\} \ ,$$

with right to left composition as usual.

Of course, $|G| = 6$.



Exercise. Write out the multiplication table for G. Remember that fg means first apply the isometry g to the triangle, then the isometry f.

2. **Permutations**: label the vertices of the triangle $1, 2, 3$. Since each isometry of the plane is determined by its effect on this triangle, we can unambiguously track the isometries via permutations of $\{1, 2, 3\}$. We obtain the permutation group

$$S_3 = \{(\,), (1,2,3), (1,3,2), (2,3), (1,3), (1,2)\}$$

(again composed right to left as functions).

We have seen that $G \simeq S_3$. Explicitly, there is an isomorphism mapping

$$\begin{array}{rcl} G & \to & S_3 \\ 1 & \mapsto & (\,) \\ s_1 & \mapsto & (1,2,3) \\ s_2 & \mapsto & (1,3,2) \\ r_1 & \mapsto & (2,3) \\ r_2 & \mapsto & (1,3) \\ r_3 & \mapsto & (1,2) \end{array}$$

3. **Matrices (version 1) : orthogonal**. Place the origin O at the centre of the triangle. Thus every symmetry of the triangle fixes O.

   Compute relative to the usual **orthonormal** basis. After rescaling the triangle, we may assume that the top vertex is

$$\vec{e_2} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad .$$

   As usual,

$$\vec{e_1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

   is the unit vector pointing east. We then get a matrix group $M1$ in which the above isometries are represented in order as

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix}, \begin{bmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{bmatrix},$$

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix}, \begin{bmatrix} 1/2 & -\sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{bmatrix} \quad .$$

   Here each matrix is orthogonal: to get the inverse, simply transpose.

4. **Matrices (version 2) : nice but not orthogonal**

   We can actually employ any basis that we want. But it makes sense to choose a 'nice' basis. So let's take vertices 1 and 2 of the triangle as the new basis vectors $\vec{d_1}$ and $\vec{d_2}$. Because the triangle is equilateral, we see that vertex 3 is given by $-\vec{d_1} - \vec{d_2}$. A little computation gives a new set $M2$ of matrices for the original isometries, again in the original order:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad .$$

   Thus the entries of these new matrices are a little nicer to work with.

   We have the same group, of course; but since the basis is non-standard, the corresponding coordinates are non-standard and measurement works differently. For example, the usual inner product $x_1y_1 + x_2y_2$ using new coordinates *does not* usefully measure anything.

5. The **trace** of a square matrix A is the sum of its diagonal entries, say

$$\mathrm{tr(A)} := \sum_{\mathrm{j}} \mathrm{a_{jj}} \quad .$$

   Thus the trace of a matrix is a very special scalar.

   Notice that corresponding matrices in the above groups have identical traces. Why is this so?

Well, we have changed basis according to this rule:

$$\vec{d_1} = \vec{e_2} = 0\vec{e_1} + 1\vec{e_2} \ , \ \ \vec{d_2} = (-\sqrt{3}/2)\vec{e_1} + (-1/2)\vec{e_2} \ .$$

Thus the corresponding *basis change matrix* is

$$B = \begin{bmatrix} 0 & -\sqrt{3}/2 \\ 1 & -1/2 \end{bmatrix} \ .$$

Symbolically we should think

$$(\text{new basis } \vec{d_1}, \vec{d_2} \text{ in a row}) = (\text{old basis } \vec{e_1}, \vec{e_2} \text{ in a row}) \ B$$

It follows that if A is one of the six 'old' matrices in $M1$, then the corresponding 'new' matrix in $M2$ is

$$B^{-1}AB \ .$$

Remark: the exact arrangement of matrices here is a little tricky. Of course, much the same procedure works in n dimensions.

Let's return to the traces. It is easy to check for square $n \times n$ matrices A and C that

$$\mathrm{tr(AC)} = \mathrm{tr(CA)} \ .$$

(Do this as an exercise.) Thus

$$\begin{aligned} \mathrm{tr(B^{-1}(AB))} &= \mathrm{tr((AB)B^{-1})} \\ &= \mathrm{tr(A(BB^{-1}))} \\ &= \mathrm{tr(A(I))} \\ &= \mathrm{tr(A)} \ . \end{aligned}$$

In short, basis change does not change the trace values for matrix group representations of the original group G.

These trace values are called the **character values** for the matrix representation. Indeed, they serve to classify and distinguish essentially different matrix representations for one and the same group G.

In a sense, the character values (traces) contain just enough numerical information to completely determine the matrix group (up to a change in basis). All other numerical data in the matrices is clutter.

6. **Exercise**. Prove that conjugate elements in G must have identical character values.

   The upshot, which is quite hard to prove, is that a matrix group is determined by k scalars, where k is the **class number** = number of conjugacy classes in G.

7. **The first level of abstraction: the mutiplication table of** G: In a basic way, the multiplication table alone completely defines G, though we must of course inspect the table to root out the interesting properties of G. In this abstract point of view, we forget all concrete representations such as isometries, permutations, matrices, etc. and think merely of $|G|$ symbols combined according to the table.

	$\mathbf{1}$	$\mathbf{s_1}$	$\mathbf{s_2}$	$\mathbf{r_1}$	$\mathbf{r_2}$	$\mathbf{r_3}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{s_1}$	$\mathbf{s_2}$	$\mathbf{r_1}$	$\mathbf{r_2}$	$\mathbf{r_3}$
$\mathbf{s_1}$	$\mathbf{s_1}$	$\mathbf{s_2}$	$\mathbf{1}$	$\mathbf{r_3}$	$\mathbf{r_1}$	$\mathbf{r_2}$
$\mathbf{s_2}$	$\mathbf{s_2}$	$\mathbf{1}$	$\mathbf{s_1}$	$\mathbf{r_2}$	$\mathbf{r_3}$	$\mathbf{r_1}$
$\mathbf{r_1}$	$\mathbf{r_1}$	$\mathbf{r_2}$	$\mathbf{r_3}$	$\mathbf{1}$	$\mathbf{s_1}$	$\mathbf{s_2}$
$\mathbf{r_2}$	$\mathbf{r_2}$	$\mathbf{r_3}$	$\mathbf{r_1}$	$\mathbf{s_2}$	$\mathbf{1}$	$\mathbf{s_1}$
$\mathbf{r_3}$	$\mathbf{r_3}$	$\mathbf{r_1}$	$\mathbf{r_2}$	$\mathbf{s_1}$	$\mathbf{s_2}$	$\mathbf{1}$

8. **The second and universal level of abstraction: a presentation for** G. Intuitively, a *presentation* for a group G is a 'concise' summary of the multiplication table, basically a minimal amount of information which would suffice to reconstruct the whole table. Note that this means that

   - we should be able to reconstruct all elements of the group; and
   - we should be able to say how all elements multiply.

   Now let's be more precise. What we require in a presentation is

   (a) a (preferably small) set of **generators** $a, b, c, \ldots$ for the group G. This means that *every* element $g \in G$ is a product of these generators or their inverses, allowing repeats. Such a product is often called a **word** in the generators. Examples are $a, aa^{-1}, abaaab^{-1}b^{-1}cc$ etc. Of course, these can sometimes be simplified using the basic laws of exponents valid for *all* groups:

   $$aa^{-1} = 1 \ , \ abaaab^{-1}b^{-1}cc = aba^3b^{-2}c^2 \ .$$

   But there could well be other simplifications possible due to special features of the group G in question. These peculiarities are given by

   (b) a set of **relations** (a.k.a. relators) satisfied by the given generators and from which all valid relations in G follow by algebraic manipulations in the group. This is a little hard to define more precisely, so here we will just sketch a few examples and state the key theorems.

9. **Example**. Suppose in the calculation just above, we do know that $ab = ba$, which can be rewritten as $aba^{-1}b^{-1} = 1$. Then we achieve a further simplification:

   $$abaaab^{-1}b^{-1}cc = a^4b^{-1}c^2 \ .$$

10. **Example**. Suppose G is generated by *two* elements a, b which satisfy the relations

$$a^2 = b^2 = (ab)^3 = 1 \qquad (**)$$

Various different groups have these generators and satisfy the relations!!

(a) $a = b = 1$ (say the integer 1); so $G = \{1\}$ has order 1.

(b) $a = b = -1$ (again integers). Check that the relations (**) are satisfied. What now is the order of G?

(c) Another possibility using ordinary integers? $a = 1$ and $b = -1$. Are all the relations (**) above satisfied?

(d) Now try the symmetry group of the equilateral triangle above. Let $a =$? and $b =$? be carefully chosen symmetries. Do they generate the full symmetry group? Do they satisfy the relations (**)?
Hint: your choices for a and b will be closely guided by the relations to be satisfied.

(e) Thus the order of G could be as big as 6. Could it be larger still? Try to compute the possibilities!! Take all possible combinations of a, b, a^{-1}, b^{-1}, subject to the relations (**), and determine how many truly different elements you can get. For example, $a^2 = 1$ implies $a^2a^{-1} = 1a^{-1}$, so that $a = a^{-1}$. In short, *in this example*, negative poweres of the generators are unnecessary, and at the outset, we can restrict only to positive integral exponents.

(f) In fact, there is a *largest such group* satisfying (**) !! And its order is _____

Remark: the peculiar structure of the relations in (**) means that the symmetry group of the equilateral triangle is the *Coxeter group* of type A_2.

11. **Theorem**. Consider all groups generated by generators

$$a, b, c \ldots$$

satisfying specified relations

$$w_1 = w_2 = \ldots = 1$$

(namely certain special words in the generators).

Then there exists a 'largest' such group, denoted

$$G = \langle a, b, c \ldots \mid w_1 = w_2 = \ldots = 1 \rangle$$

(This is called a *presentation* for the group G.)

More precisely, if H is any other group with corresponding generators $\tilde{a}, \tilde{b}, \tilde{c} \ldots$ satisfying the corresponding relations $\tilde{w}_1 = \tilde{w}_2 = \ldots = \tilde{1}$, then there exists a unique homomorphism

$$\varphi : G \to H$$

which explicitly sends a to $\tilde{a}$, b to $\tilde{b}$, etc.

12. **Remarks**.

(a) This is a very powerful theorem. For example, it says that we can construct groups at will, choosing random symbols for generators, random equations for relations. Of course, the resulting groups could be trivial (order 1), could be infinite, could be uninteresting.

(b) Recall that $H \simeq G/\ker\varphi$. Hence,

$$|G| = |H| \, |\ker\varphi| \, .$$

Since $|H|$ divides $|G|$, we do indeed find that $|G| \geqslant |H|$. In this sense, G is the largest group satisfying the relations. (It could be infinite.)

(c) It is a nice exercise to use the theorem to prove that G is uniquely defined up to isomorphism.

13. **Exercises on presentations**. Compute the orders of these groups and describe each in more familiar terms (e.g. symmetry group of equilateral triangle).

    (a) $G = \langle a \,|\, a^2 = 1 \rangle$

    (b) $G = \langle b \,|\, b^3 = 1 \rangle$

    (c) $G = \langle a, b \,|\, a^2 = b^2 = (ab)^4 = 1 \rangle$

    (d) $G = \langle a, b \,|\, a^2 = b^4 = aba^{-1}b^{-1} = 1 \rangle$

    (e) $G = \langle a, b, c \,|\, a^2 = b^2 = c^2 = (ab)^3 = (bc)^3 = (ac)^2 = 1 \rangle$

    (f) $G = \langle a, b \,|\, a^2 = b^2 = (ab)^2 \rangle$
    Warning: we aren't saying $a^2 = 1$ here; rather, the relations are just clean ways of writing

    $$a^2 b^{-2} = a^2 (ab)^{-2} = 1 \ .$$

    It is still possible, for example, that a has infinite period!!

    (g) $G = \langle a, b \,|\, a^2 = b^2 = 1 \rangle$

    (h) $G = \langle a, b \,|\, a^3 = b^3 = (ab)^3 = 1 \rangle$

13 Conjugacy and Characters

Here are several exercises to bolster your understanding of conjugacy and and characters. Try to construct your own proofs before consulting a standard text.

Usually

G will be a general finite group, its order denoted by $|G|$. Its identity will usually be e.

1. Recall that b **is conjugate to** c in a group G if $b = gcg^{-1}$ for some $g \in G$. Let us indicate this by
$$b \sim c$$

   Theorem. $\sim$ is an equivalence relation.

   Proof. Supply details:

   □

2. Thus each element $b \in G$ belongs to a unique equivalence class, called naturally a **conjugacy class**. Let's denote this class by $\mathrm{Cl}(b)$. Thus, $|\mathrm{Cl}(b)|$ is the number of elements of G which are conjugate to b (including b itself, of course).

3. **Remarks for Discussion**: when G is a geometrical group, the conjugacy classes correspond to 'geometrically distinct' kinds of isometries. For example, for an ordinary square the rotational symmetries and the reflections lie in different conjugacy classes. In fact, the reflections themselves split into two distinct conjugacy classes. What are they?

   In the full permutation group S_n, the conjugacy classes correspond to the essentially different ways of writing n as a sum of positive integers.

4. Suppose a group G has k conjugacy classes. Choose at random an element b_j in the jth class.

   Exercises.

   (a) One such class representative is forced. Which is it and how big is that conjugacy class?

   (b) Simplify

$$\sum_{j=1}^{k} |\mathrm{Cl}(b_j)| = \_\_\_\_\_$$

5. Fix an element $b \in G$. Then the **centralizer** of b in G is the set of all elements of G which commute with b:

$$C(b) := \{g \in G \,|\, gb = bg\} \quad .$$

   Theorem. $C(b)$ is a subgroup of G.

   Proof. Supply details concerning identity e, closure under inverse, products.

□

6. **Exercises**.

   (a) What is $C(e)$?

   (b) Show that always $b \in C(b)$. Ditto for b^{-1}, in fact for any b^n, where $n \in \mathbb{Z}$.

7. **Theorem**. Suppose $b = gcg^{-1}$ (so that $b \sim c$). Then

$$C(b) = g\,C(c)\,g^{-1} \ .$$

Remark: thus conjugate elements have conjugate centralizers. Two such groups must be isomorphic, and so have the same size.

Proof. Supply details. □

Now for the really neat theorem!!

8. **Theorem**. The number of conjugates of b in G equals the index of the centralizer of B:

$$|\mathrm{Cl}(b)| = [G \,:\, C(b)] \ .$$

Hence, the number of elements in a conjugacy class divides the order of the group.

Proof. Fix $b \in G$. Put the left cosets of $C(b)$ into a set

$$LC := \{g\,C(b) \,:\, g \in G\}$$

Remember that in a set we count only distinct elements. Thus

$$|LC| = \frac{|G|}{|C(b)|} = t \ \text{(say)}.$$

It is not useful here, but one could choose explicit coset representatives $g_1, \ldots, g_t$, so that the different cosets in LC would then be $g_1C(b), \ldots, g_tC(b)$.

Define

$$\begin{array}{rcl} \varphi : \mathrm{Cl}(b) & \to & LC \\ gbg^{-1} & \mapsto & gC(b) \end{array}$$

Supply details that φ is well-defined, onto and 1–1.

□

9. **Exercises**.

(a) Let $G = S_4$, with standard generators $r_1 = (1\,2), r_2 = (2\,3), r_3 = (3\,4)$. Fill in the data in the following table:

Class Rep. b	Factorization of b in terms of the r_j's	Size $C(b)$	$\frac{\lvert G\rvert}{\lvert C(b)\rvert}$	Explicit list of conjugates
()				
(1 2)				
(1 2)(3 4)				
(1 2 3)				
(1 2 3 4)				

(b) Do the same thing for S_5, say with generators $r_1 = (1\,2), r_2 = (2\,3), r_3 = (3\,4)$ and $r_4 = (4\,5)$.

You needn't however explicitly list the conjugates.

(c) How many conjugacy classes does S_6 have?

(d) Let G be the symmetry group of a cube. What is $|G|$? How many conjugacy classes does G have and what are their sizes?