1.2 The axioms of a group

It's time now to consider the formal definition of a group. After this you should carefully check that each of the examples in Section 1.1 *is* indeed a group, and identify in each case the identity element and the inverse of a typical element. The formal definition is stated below followed by some explanatory notes.

Definition 1.2.1. *A* group G *is a non-empty set equipped with a binary operation* $\star$*, in which the following axioms hold.*

1. $\star$ *is an* associative operation. *This means that for any elements* x, y, z *of* G
$$(x \star y) \star z = x \star (y \star z).$$
2. *Some element* id *of* G *is an* identity element *for* $\star$*. This means that for every element* x *of* G
$$\mathrm{id} \star x = x \star \mathrm{id} = x.$$
3. *For every element* x *of* G *there is an element* x^{-1} *of* G *that is an* inverse *of* x *with respect to* $\star$*.*

Notes

1. *The first line of the definition*
A binary operation on a set G is a way of combining two elements of G (in specified order) to produce a new element of G. Technically it is a function from G $\times$ G (the set of ordered pairs of elements of G) to G. For example:
   - Addition is a binary operation on the set $\mathbb{N}$ of natural numbers.
   - Subtraction is *not* a binary operation on $\mathbb{N}$. *Why not*?
   - Matrix multiplication is a binary operation on the set $M_3(\mathbb{Q})$ of 3×3 matrices with rational entries (but not on the set of *all* square matrices with rational entries - why?).

   Implicit in the statement that $\star$ is a binary operation on G is the condition that when you use $\star$ to combine two elements of G, the result is again an element of G, i.e. that G is *closed* under $\star$. Some authors list this as one of the axioms of a group - you may see this in some books.

2. *Associativity* is a property that some operations have and that some do not. Our first axiom says that in order for a structure to be considered a group, its binary operation must be associative. People do consider algebraic structures that have non-associative operations, the most commonly encountered examples are *Lie Algebras*.
Exercise: Give an example of a familiar binary operation (on $\mathbb{Z}$ for example) that is not associative.

3. An identity element for a binary operation is sometimes referred to as a *neutral element*, a term which is probably more self-explanatory although less prominent. An identity element for a binary operation $\star$ is one that has no effect on any element when combined with that element using $\star$. For example, 0 is an identity element for addition in $\mathbb{Z}$, 1 is an identity element for multiplication in $\mathbb{Z}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is an identity element for multiplication of 2×2 matrices.
Important exercise: In each of the examples in Section 1.1, identify the identity element.

4. If we have an identity element for some binary operation, we can consider whether certain elements have *inverses* or not. Two elements x and y are *inverses* of each other with respect to the binary operation $\star$ if $x \star y$ and $y \star x$ are both equal to the identity element. For example, -5 and 5 are inverses for each other with respect to addition in $\mathbb{Z}$; this means that adding -5 to some integer "reverses" the work of adding 5. The rational numbers $\frac{2}{5}$ and $\frac{5}{2}$ are inverses of each other for multipication in $\mathbb{Q}$; this means we can "undo" the work of multiplying by $\frac{5}{2}$ if we multiply by $\frac{2}{5}$. Of course we could describe these examples in terms of subtracting

and dividing, but it is helpful to get used to thinking in terms of inverses if you can, we will not always have notions of subtraction and division. It is entirely possible for an element to be its own inverse - this is the case for the identity element of every group, and also for example for the reflections in D_6 or for the element $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ of $GL(2, \mathbb{Q})$.

Important exercise: In each of the examples in Section 1.1, identify the inverse of a typical element.

Note: In order to talk about inverses, you must have a particular binary operation in mind and your set must have an identity element for that operation.

Definition 1.2.1 is the criterion that decides whether a given algebraic structure is a group or not.

Problem 1.2.2. *Let* $UT_3(\mathbb{Q})$ *be the set of* 3×3 *upper triangular matrices with rational entries. Is* $UT_3(\mathbb{Q})$ *a group under matrix multiplication?*

Recall that a square matrix A is *upper triangular* if all entries below its main diagonal are zeros (or equivalently if $A_{ij} = 0$ whenever $i > j$). To answer this question you must ask yourself:

- Is $UT_3(\mathbb{Q})$ closed under matrix multiplication?
- Is the operation associative? (In most examples of interest the answer is yes as in this case - multiplication of $n \times n$ matrices is always associative).
- Does this set contain an identity element for the operation? (In this example this question amounts to whether the identity element for multiplication of 3×3 matrices is upper triangular).
- Does every element of the set have an inverse that belongs to the set?

To confirm that your object is a group, you need to check that all of these questions have a positive answer. If you find that one of them has a negative answer, that is enough to justify the conclusion that your object is not a group. The answer is no in the case of Problem 1.2.2. Why?

Problem 1.2.3. *Let* S *be the set of* 3×3 *upper triangular matrices with rational entries, in which no element has a zero entry on the main diagonal. Is* S *a group under matrix multiplication?*

We conclude this section by mentioning two obvious and important dichotomies in group theory. Definition 1.2.1 says that a group must be a non-empty set but says nothing about how many elements it can have. A group is called *infinite* if it has infinitely many elements and *finite* if it has finitely many elements. The study of infinite groups tends to have quite a different flavour from the study of finite groups, essentially because in the later case we can do things like count elements (in the whole group or in a subset of interest).

Exercise Determine which of the examples in Section 1.1 are finite.

Recall that a binary operation $\star$ on a set S is *commutative* if

$$x \star y = y \star x$$

for all elements x, y of S. There is nothing in Definition 1.2.1 requiring that a group operation be commutative. A group whose operation *is* commutative is called *abelian*, after the Norwegian mathematician Niels Henrik Abel (1802–1829).

Exercise Determine which of the examples in Section 1.1 are abelian.
For example, the multiplicative group $\mathbb{C}^\times$ (or$(\mathbb{C}^\times, \times)$) of the complex numbers is abelian, but $GL(2, \mathbb{Q})$ is not.

Remark on Notation: Especially in the non-abelian case, the identity element of a group is often referred to as 1 (whether it is the *number* 1 or not) and the result of combining the elements a and b with the group operation is often just written ab - i.e. there is no particular symbol like $\times$ or $\circ$

or whatever used within the product. This is just a notational convention and worth getting used to - it makes writing simpler when you do get used to it.

Abelian groups are often written with the operation referred to as *addition* and denoted $+$, and the identity element denoted as 0. This makes sense of course if the operation naturally is a version of addition (of numbers, matrices or functions for example), but sometimes the additive notation is also used in an abstract context. The symbol "$+$" would never conventionally be used for a non-commutative operation.

Remark on History: The modern definition of a group (Definition 1.2.1) is nowadays a starting point for the study of group theory. It was not the starting point in the development of the subject although it was a significant milestone. The first abstract definition of a group was given by Arthur Cayley in 1854. This arose from several decades of work on what are now called groups of permutations and on solving polynomial equations by Lagrange, Abel and Galois among others, and on groups of symmetries in geometry by Klein. The introduction of an abstract definition brought the subject into its modern form and had a massive impact on the development of algebra.