

## Lecture 4: The axioms of a group (Section 1.2)

### Definition

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  $\text{id}$  of  $G$  is an *identity element* for  $\star$ . This means that for every element  $x$  of  $G$

$$\text{id} \star x = x \star \text{id} = x.$$

3. For every element  $x$  of  $G$  there is an element  $x^{-1}$  of  $G$  that is an *inverse* of  $x$  with respect to  $\star$ .

## A group $G$ is a non-empty set equipped with a binary operation $\star$

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  $3 \times 3$  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  $\star$ .

# Associativity

- ▶ **Associativity** is a property that some operations have and that some do not.
- ▶ A binary operation combines elements in **pairs**. It can combine three elements by combining one (consecutive) pair first and then combining the result of that with the third (without changing the overall order of the three). The operation  $\star$  is associative if

$$(x \star y) \star z = x \star (y \star z)$$

for all elements  $x, y, z$ .

- ▶ Another way to say this is that  $\star$  is associative if the expression  $x \star y \star z$  is unambiguous.
- ▶ An example of an operation that's not associative is subtraction on  $\mathbb{Z}$ :  $(3 - 5) - 6 \neq 3 - (5 - 6)$ .

## Identity element (neutral element)

- ▶ 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 (on the left or right) 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  $2 \times 2$  matrices.

# Inverses

- ▶ If (and only 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, the rational numbers  $\frac{2}{5}$  and  $\frac{5}{2}$  are inverses of each other for multiplication in  $\mathbb{Q}$ ; this means we can “undo” the work of multiplying by  $\frac{5}{2}$  if we multiply by  $\frac{2}{5}$ .
- ▶ In a group, the binary operation must have an identity element, and every element must have an inverse within the group. It is possible for an element to be its own inverse.

## An example

Let  $UT_3(\mathbb{Q})$  be the set of  $3 \times 3$  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. To answer the 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  $3 \times 3$  matrices is upper triangular).
- ▶ Does every element of the set have an inverse that belongs to the set?

Abelian or non-Abelian, finite or infinite?