

2. DEFINITION OF A GROUP

Definition 2.1. A group is a set G together with a binary operation (written as juxtaposition)

$$\begin{aligned} G \times G &\rightarrow G \\ (g, h) &\mapsto gh \end{aligned}$$

satisfying the following axioms.

Gp1: (associativity) $a(bc) = (ab)c \quad \forall a, b, c \in G$

Gp2: (identity) G has an identity e so that

$$ge = eg = g \quad \forall g \in G$$

Gp3: (inverse) Every $g \in G$ has an inverse h so that

$$gh = hg = e$$

2.1. consequences of the axioms.

Theorem 2.2. The identity in any group is unique.

Theorem 2.3. The inverse of any element is unique.

Proof. Someone suggested the following: If h, h' are both inverses of g then

$$gh = e = gh'$$

Now cancel g to get $h = h'$. □

For this argument to work we need:

Lemma 2.4. (left cancellation) If $gx = gy$ then $x = y$. Similarly, (right cancellation) If $xg = yg$ then $x = y$.

Proof. Multiplying both sides by the inverse:

$$h(gx) = (hg)x = ex = x$$

is equal to

$$h(gy) = (hg)y = ey = y$$

So, $x = h(gx) = h(gy) = y$. (This uses the axiom of equality which says that if $A = B$ then any statement about A is also true for B . Here the statement “ $hA = x$ ” is true for $A = gx$. Therefore it is also true for $A = gy$.) □

Since the inverse of g is unique, we denote it by g^{-1} .

2.2. examples of groups. I asked the class for example of groups and I got some surprising answers. One interesting suggestion was the set $\{0, 1, -1\}$ under multiplication. This almost works, the only flaw is that 0 does not have an inverse. As you will learn shortly, there is only one group of order 3 up to isomorphism and this is not it.