

Let  $G$  and  $H$  be groups and let  $f : G \rightarrow H$  map elements of  $G$  to elements of  $H$ .

$f$  is *injective* if  $f$  is one-to-one. i.e.,  $f(a) = f(b) \Rightarrow a = b$ .  $f : G \rightarrow H$ .

$f$  is *surjective* (onto) if  $\forall b \in H \exists a \in G \ni f(a) = b$ .  $f : G \rightarrow H$

$f$  is a *bijection* if it is injective and surjective.  $f : G \rightarrow H$ .

$f$  is a homomorphism if  $f(ab) = f(a)f(b)$ .

An injective homomorphism is a *monomorphism*

A surjective homomorphism is an *epimorphism*

A bijective homomorphism is an *isomorphism*. In this case  $G$  and  $H$  are said to be *isomorphic*  $G \simeq H$ .

If  $H = G$ , then homomorphism is called an *endomorphism*.

If  $H = G$ , then an isomorphism is called an *automorphism*.

**1** Let  $Q_8$  be the group generated by ordinary matrix multiplication by the complex matrices  $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  and  $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ , where  $i^2 = -1$ . Show that  $Q_8$  is a non-Abelian group of order 8.

**2** Let  $H$  be the group generated by ordinary matrix multiplication by the real matrices  $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  and  $D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . Show that  $H$  is a non-Abelian group of order 8. Show that this group is not isomorphic to the group found in **1**.

**3** Construct another group of size 8. i.e., one not isomorphic to either of the groups found in **1** and **2**.

**4** Let  $S$  be a nonempty subset of a group  $G$  and define a relation on  $G$  by  $a \sim b$  iff  $a \otimes b^{-1} \in S$ . Show that  $\sim$  is an equivalence relation if and only if  $S$  is a subgroup of  $G$ . A subset of a group is a subgroup if it is a group under the binary operation inherited from the group.

**5** Let  $f : G \rightarrow H$  be a homomorphism of groups,  $A$  a subgroup of  $G$ , and  $B$  a subgroup of  $H$ .

(A) Show that  $\text{Ker } f$  and  $f^{-1}(B)$  are subgroups of  $G$ .

(B) Show that  $f(A)$  is a subgroup of  $H$ .

**6** Let  $G$  be a group and  $\text{Aut}(G)$  be the set of all automorphisms of  $G$ . Show that  $\{\text{Aut}(G), \text{composition of functions}\}$  is a group

**7** Show that  $\text{Aut}(\mathbf{Z}) \simeq \mathbf{Z}_2$ , where  $Z_m$  is the set of congruence classes modulo  $m$ .

**8** (2.12) (A) For any elliptic curve  $E$  in Weierstrass form, Show that  $(x, y) \mapsto (x, -y)$  is a group homomorphism from  $E$  to itself.

(B) Show that  $(x, y) \mapsto (\zeta x, y)$ , where  $\zeta$  is a nontrivial cube root of 1, is an automorphism of the elliptic curve  $E : y^2 = x^3 + B$ .

(C) Show that  $(x, y) \mapsto (-x, iy)$ , where  $i^2 = -1$ , is an automorphism of the elliptic curve  $y^2 = x^3 + Ax$ .