

when each s_i is replaced by r_i . Then there is a (unique) homomorphism $\varphi : G \rightarrow H$ which maps s_i to r_i . If we have a presentation for G , then we need only check the relations specified by this presentation (since, by definition of a presentation, every relation can be deduced from the relations given in the presentation). If H is generated by the elements $\{r_1, \dots, r_m\}$, then φ is surjective (any product of the r_i 's is the image of the corresponding product of the s_i 's). If, in addition, H has the same (finite) order as G , then any surjective map is necessarily injective, i.e., φ is an isomorphism: $G \cong H$. Intuitively, we can map the generators of G to any elements of H and obtain a homomorphism provided that the relations in G are still satisfied.

Readers may already be familiar with the corresponding statement for vector spaces. Suppose V is a finite dimensional vector space of dimension n with basis S and W is another vector space. Then we can specify a linear transformation from V to W by mapping the elements of S to arbitrary vectors in W (here there are no relations to satisfy). If W is also of dimension n and the chosen vectors in W span W (and so are a basis for W) then this linear transformation is invertible (a vector space isomorphism).

Examples

- (1) Recall that $D_{2n} = \langle r, s \mid r^n = s^2 = 1, sr = r^{-1}s \rangle$. Suppose H is a group containing elements a and b with $a^n = 1$, $b^2 = 1$ and $ba = a^{-1}b$. Then there is a homomorphism from D_{2n} to H mapping r to a and s to b . For instance, let k be an integer dividing n with $k \geq 3$ and let $D_{2k} = \langle r_1, s_1 \mid r_1^k = s_1^2 = 1, s_1r_1 = r_1^{-1}s_1 \rangle$. Define

$$\varphi : D_{2n} \rightarrow D_{2k} \quad \text{by} \quad \varphi(r) = r_1 \text{ and } \varphi(s) = s_1.$$

If we write $n = km$, then since $r_1^k = 1$, also $r_1^n = (r_1^k)^m = 1$. Thus the three relations satisfied by r, s in D_{2n} are satisfied by r_1, s_1 in D_{2k} . Thus φ extends (uniquely) to a homomorphism from D_{2n} to D_{2k} . Since $\{r_1, s_1\}$ generates D_{2k} , φ is surjective. This homomorphism is not an isomorphism if $k < n$.

- (2) Following up on the preceding example, let $G = D_6$ be as presented above. Check that in $H = S_3$ the elements $a = (1\ 2\ 3)$ and $b = (1\ 2)$ satisfy the relations: $a^3 = 1$, $b^2 = 1$ and $ba = ab^{-1}$. Thus there is a homomorphism from D_6 to S_3 which sends $r \mapsto a$ and $s \mapsto b$. One may further check that S_3 is generated by a and b , so this homomorphism is surjective. Since D_6 and S_3 both have order 6, this homomorphism is an isomorphism: $D_6 \cong S_3$.

Note that the element a in the examples above need not have *order* n (i.e., n need not be the *smallest* power of a giving the identity in H) and similarly b need not have order 2 (for example b could well be the identity if $a = a^{-1}$). This allows us to more easily construct homomorphisms and is in keeping with the idea that the generators and relations for a group G constitute a complete set of data for the group structure of G .

EXERCISES

Let G and H be groups.

1. Let $\varphi : G \rightarrow H$ be a homomorphism.

- (a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.
 (b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

- If $\varphi : G \rightarrow H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?
- If $\varphi : G \rightarrow H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \rightarrow H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H ?
- Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.
- Prove that the additive groups \mathbb{R} and \mathbb{Q} are not isomorphic.
- Prove that the additive groups \mathbb{Z} and \mathbb{Q} are not isomorphic.
- Prove that D_8 and Q_8 are not isomorphic.
- Prove that if $n \neq m$, S_n and S_m are not isomorphic.
- Prove that D_{24} and S_4 are not isomorphic.

- Fill in the details of the proof that the symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$ as follows: let $\theta : \Delta \rightarrow \Omega$ be a bijection. Define

$$\varphi : S_\Delta \rightarrow S_\Omega \quad \text{by} \quad \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \quad \text{for all } \sigma \in S_\Delta$$

and prove the following:

- φ is well defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω .
- φ is a bijection from S_Δ onto S_Ω . [Find a 2-sided inverse for φ .]
- φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

Note the similarity to the *change of basis* or *similarity* transformations for matrices (we shall see the connections between these later in the text).

- Let A and B be groups. Prove that $A \times B \cong B \times A$.
- Let A , B , and C be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C \cong A \times H$.
- Let G and H be groups and let $\varphi : G \rightarrow H$ be a homomorphism. Prove that the image of φ , $\varphi(G)$, is a subgroup of H (cf. Exercise 26 of Section 1). Prove that if φ is injective then $G \cong \varphi(G)$.
- Let G and H be groups and let $\varphi : G \rightarrow H$ be a homomorphism. Define the *kernel* of φ to be $\{g \in G \mid \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H , i.e., is the fiber over the identity of H). Prove that the kernel of φ is a subgroup (cf. Exercise 26 of Section 1) of G . Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G .
- Define a map $\pi : \mathbb{R}^2 \rightarrow \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf. Exercise 14).
- Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \rightarrow A$ and $\pi_2 : G \rightarrow B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels (cf. Exercise 14).
- Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.
- Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.
- Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

20. Let G be a group and let $\text{Aut}(G)$ be the set of all isomorphisms from G onto G . Prove that $\text{Aut}(G)$ is a group under function composition (called the *automorphism group* of G and the elements of $\text{Aut}(G)$ are called *automorphisms* of G).
21. Prove that for each fixed nonzero $k \in \mathbb{Q}$ the map from \mathbb{Q} to itself defined by $q \mapsto kq$ is an automorphism of \mathbb{Q} (cf. Exercise 20).
22. Let A be an abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$ prove that this homomorphism is an isomorphism (i.e., is an automorphism of A).
23. Let G be a finite group which possesses an automorphism σ (cf. Exercise 20) such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G , prove that G is abelian (such an automorphism σ is called *fixed point free* of order 2). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]
24. Let G be a finite group and let x and y be distinct elements of order 2 in G that generate G . Prove that $G \cong D_{2n}$, where $n = |xy|$. [See Exercise 6 in Section 2.]
25. Let $n \in \mathbb{Z}^+$, let r and s be the usual generators of D_{2n} and let $\theta = 2\pi/n$.
- Prove that the matrix $\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ is the matrix of the linear transformation which rotates the x, y plane about the origin in a counterclockwise direction by θ radians.
 - Prove that the map $\varphi : D_{2n} \rightarrow GL_2(\mathbb{R})$ defined on generators by
- $$\varphi(r) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \quad \text{and} \quad \varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
- extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$.
- Prove that the homomorphism φ in part (b) is injective.
26. Let i and j be the generators of Q_8 described in Section 5. Prove that the map φ from Q_8 to $GL_2(\mathbb{C})$ defined on generators by
- $$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \quad \text{and} \quad \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
- extends to a homomorphism. Prove that φ is injective.

1.7 GROUP ACTIONS

In this section we introduce the precise definition of a group acting on a set and present some examples. Group actions will be a powerful tool which we shall use both for proving theorems for abstract groups and for unravelling the structure of specific examples. Moreover, the concept of an “action” is a theme which will recur throughout the text as a method for studying an algebraic object by seeing how it can act on other structures.

Definition. A *group action* of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

- (1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$, and
- (2) $1 \cdot a = a$, for all $a \in A$.