First isomorphism theorem, and symmetries of a cube

In this lecture we prove the "1st Isomorphism Theorem" and discuss some consequences. We also explore the rotational symmetries of a cube in 3-dimensional Euclidean space.

▶ **1st Isomorphism Theorem: Let $\phi : G \to G'$ be an *onto* homomorphism. Then there is a naturally induced map which we write as**

$$\psi : G/\mathbf{ker}(\phi) \longrightarrow G'$$

and this map ψ is an isomorphism of groups.

Proof. Write $N = \ker(\phi)$. Define the map ψ as follows: for any coset $aN \in G/N$ we let $\psi(aN) = \phi(a)$. Let us check this is well-defined. Suppose $aN = bN$. This means $ab^{-1} \in N$, i.e. $e' = \phi(ab^{-1}) = \phi(a)\phi(b)^{-1}$. Thus $\phi(a) = \phi(b)$. In particular,

$$\phi(a) = \psi(aN) = \psi(bN) = \phi(b)$$

This tells us ψ is well-defined map, independent of how the coset aN is written.

Next, we check ψ is a homomorphism. For $aN, bN \in G/N$ we simply compute

$$\psi(aN)\psi(bN) = \phi(a)\phi(b) = \phi(ab) = \psi(abN) = \psi(aNbN)$$

and thus ψ is a homomorphism.

Finally, we check that ψ is 1-1 and onto. Let $a' \in G'$. Because ϕ is onto, there is some $a \in G$ such that $\phi(a) = a'$. Then also $\psi(aN) = \phi(a) = a'$. Therefore ψ is onto. Finally, suppose $aN, bN \in G/N$ are such that $\psi(aN) = \psi(bN)$. This implies $\phi(a) = \phi(b)$, or $\phi(ab^{-1}) = e'$, implying $ab^{-1} \in N$. In particular, $aN = bN$. Thus ψ is 1-1, and ψ is an isomorphism. □

Examples

1. Let $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_5$ be the homomorphism given by $\phi(k \pmod{20}) = k \pmod 5$. Then $\ker(\phi) = \langle 5 \rangle \subset \mathbb{Z}_{20}$. The 1st Isomorphism Theorem gives

$$\mathbb{Z}_{20}/\langle 5 \rangle \cong \mathbb{Z}_5$$

2. Consider the exponential map $\phi : (\mathbb{R}, +) \to (U(1), \times)$, where $U(1) \subset \mathbb{C}^\times$ is the circle group, defined by $\phi(\theta) = e^{2\pi i\theta}$. This is an onto homomorphism. The kernel is

$$\ker(\phi) = \{\theta \in \mathbb{R} : e^{2\pi i\theta} = 1\} = \mathbb{Z} \subset \mathbb{R}$$

By the 1st isomorphism theorem we conclude we have an isomorphism

$$\mathbb{R}/\mathbb{Z} \cong U(1)$$

3. Consider the group of upper triangular matrices in $\mathrm{GL}_2(\mathbb{R})$ given by

$$G = \left\{ A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : \;\; a, b, c \in \mathbb{R}, \;\; ac \neq 0 \right\}$$

Define a map $\phi : G \to \mathbb{R}^\times \times \mathbb{R}^\times$ by $\phi(A) = (a, c)$. This is easily checked to be an onto homomorphism. The kernel of ϕ is given by the subgroup $H \subset G$ of upper triangular matrices with $a = c = 1$. Thus H is normal. The 1st Isomorphism Theorem gives

$$G/H \cong \mathbb{R}^\times \times \mathbb{R}^\times$$

In particular, G/H is abelian.

▸ **Let G be cyclic. If $|G| = \infty$ then $G \cong \mathbb{Z}$. If $|G|$ is finite then $G \cong \mathbb{Z}_n$ where $n = |G|$.**

Proof. Since G is cyclic, $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ for some $a \in G$. Define a map

$$\phi : \mathbb{Z} \longrightarrow G$$

by setting $\phi(k) = a^k$. Then this is onto, since a generates G. The kernel of ϕ consists of $m \in \mathbb{Z}$ such that $a^m = e$ in G. There are two cases. If G is finite, then $|G| = n$ is the order of a and $\ker(\phi) = n\mathbb{Z} \subset \mathbb{Z}$. The 1st Isomorphism Theorem gives

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker(\phi) \cong G$$

In the other case, G is infinite, and there are no m aside from $m = 0$ such that $a^m = e$, and thus the kernel of ϕ is trivial. Then $G \cong \mathbb{Z}$. □

Symmetries of a cube

Now let us turn to the group G which consists of the rotational symmetries of a cube situated in 3-dimensional Euclidean space. This group has 24 elements, as shown on the next page. We first follow a familiar strategy of describing this group: label the vertices 1 to 8, and associate to each rotation $a \in G$ a corresponding permutation $\phi(a) \in S_8$ based on how the vertices are moved around. This gives a homomorphism

$$\phi : G \longrightarrow S_8$$

This homomorphism ϕ is 1-1, but it is not onto: indeed, $|G| = 24$ but the target group S_8 has $8! = 40320$ elements.

Mapping G into S_8 is not the most ideal scenario. After all, $|S_8| = 40320$ whereas G has order only 24. A better way of representing G as a group of permutations is as follows.

There are 4 diagonal axes that pass through the cube; each one goes through two vertices that are as far apart as possible. Label these 4 diagonal axes 1, 2, 3, 4. Then for a rotation $a \in G$ we define $\psi(a) \in S_4$ to be the permutation determined by how the diagonal axes are moved around by the rotation a. This gives a homomomorphism

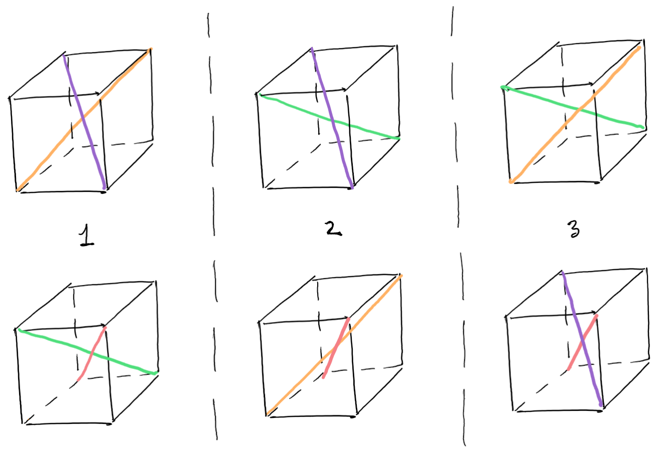
$$\psi : G \longrightarrow S_4$$

It is straightforward to verify that ψ is 1-1, i.e. that a rotation of the cube is entirely determined by how these 4 diagonal axes are permuted. Then, since $|G| = 24 = |S_4|$, we know ψ must also be onto. Therefore ψ is an isomorphism! The construction of the map ψ is illustrated on the next page.

Finally, let us return to the 1st Isomorphism Theorem. To this end, we define a map

$$\mu : S_4 \longrightarrow S_3$$

as follows. Let $\sigma \in S_4$. Then $a = \psi^{-1}(\sigma) \in G$ is a rotational symmetry of the cube. Consider the six pictures of the cube below, each with a distinguished pair of diagonal axes chosen. These six pictures of the cube are divided into 3 columns labelled $1, 2, 3$.



You may verify that the rotation a takes the two pictures in column 1 to either the two pictures in column 2, or the two pictures in column 3, and so on. Thus the columns $1, 2, 3$ above are permuted. We obtain a permutation of $\{1, 2, 3\}$ which we call $\mu(\sigma) \in S_3$. Further,

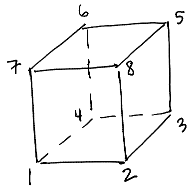
$$\ker(\mu) = H = \{e, (12)(34), (13)(24), (14)(23)\},$$

is a normal subgroup, and μ is onto. The 1st Isomorphism Theorem then tells us that

$$S_4/H \cong S_3$$

This example is actually rare: there are no homomorphisms $S_n \to S_{n-1}$ when $n > 4$!

Rotational symmetries of a cube



Original position
with vertices labelled 1–8

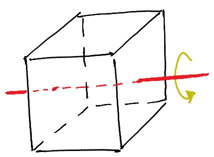
There are 24 symmetries.

By keeping track of where vertices go, we get a 1-1 homomorphism

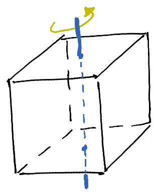
$$\left\{\begin{array}{c}\text{rotational symmetries}\\ \text{of the cube}\end{array}\right\} \longrightarrow S_8.$$

identity: corresponds to identity permutation $e \in S_8$

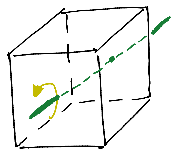
For each axis as below, get 3 nontrivial rotations:



90° (2358)(1467)
180° (25)(38)(16)(47)
270° (2853)(1764)

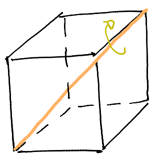


90° (1234)(5678)
180° (13)(24)(57)(68)
270° (1432)(5876)

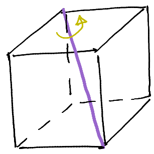


90° (1287)(5643)
180° (18)(27)(54)(63)
270° (1782)(5346)

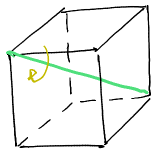
2 nontrivial rotations around each of the 4 diagonal axes:



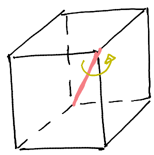
120° (386)(274)
240° (368)(247)



120° (183)(475)
240° (138)(457)

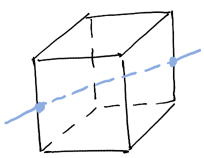


120° (168)(245)
240° (186)(254)

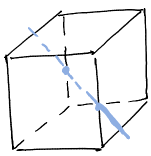


120° (257)(136)
240° (275)(163)

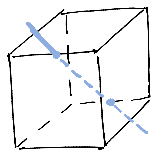
180° rotation around each edge-midpoint diagonal:



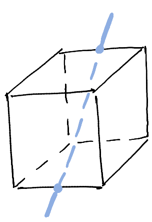
(17)(26)(35)(48)



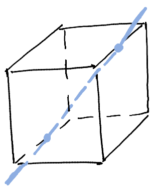
(15)(28)(37)(46)



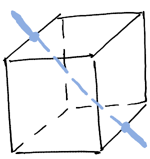
(15)(26)(34)(78)



(12)(37)(48)(56)



(14)(26)(37)(58)



(15)(23)(48)(67)