First Isomorphism Theorem

First Isomorphism Theorem

There are naturally many homomorphisms of the form $\bar{\varphi} : G \to G/\ker \bar{\varphi}$.

A more general observation can be made, namely, that the image of any homomorphism is itself a quotient group – by the kernel!

Theorem 1 (First Isomorphism Theorem)

Suppose $\varphi : G \to H$ *is a group homomorphism. Then*

$$\varphi(G) = \operatorname{image} \varphi \cong G/\ker \varphi.$$

Proof.

To simplify notation, put $K = \ker \varphi$ and use multiplicative notation to denote group operations. We shall exhibit an isomorphism; define

$$\begin{aligned} \psi : G/K &\to \varphi(G) \\ gK &\mapsto \varphi(g). \end{aligned}$$

Verifying ψ is an isomorphism is routine:

- **Claim.** ψ is well-defined.

  Proof: To show ψ is a function, we must make sure image $\psi \subset \varphi(G)$ – apparent in the definition of ψ – and that no element in G/K is mapped to two different elements in $\varphi(G)$.

Suppose $gK = hK$. By Proposition **??**, there exists $k \in K$ such that $g = hk$. By definition of the kernel, $k \in K = \ker \varphi$ implies $\varphi(k) = 1_H$, the identity element in H. Then, since by hypothesis, φ is a homomorphism,

$$\psi(gK) = \varphi(g) = \varphi(hk) = \varphi(h)\varphi(k) = \varphi(h) \cdot 1_H = \varphi(h) = \psi(hK),$$

as required. □

- **Claim.** ψ is a homomorphism.

Proof: Choose $gK, hK \in G/K$. Then

$$\begin{aligned} \psi((gK)(hK)) = \psi((gh)K) &= \varphi(gh) \\ &= \varphi(g)\varphi(h) = \psi(gK)\psi(hK), \end{aligned}$$

as required. □

- **Claim.** ψ is one-to-one.

  Proof: Suppose $\psi(gK) = \psi(hK)$. Then $\varphi(g) = \varphi(h)$. Multiply by $\varphi(h)^{-1}$:

  $$\begin{aligned} \varphi(g)\varphi(h)^{-1} &= \varphi(h)\varphi(h)^{-1} = 1_H \\ \implies \varphi(g)\varphi(h)^{-1} &= \varphi(gh^{-1}) = 1_H \\ \implies gh^{-1} &\in \ker\varphi = K. \end{aligned}$$

  Multiply by h:

  $$g = gh^{-1}h \in Kh = hK,$$

  and so by Proposition **??**, $gK = hK$. $\square$

- **Claim.** ψ is onto.

  Proof: Suppose $h \in \varphi(G)$. By definition of $\varphi(G)$, $h = \varphi(g)$ for some $g \in G$. Then $h = \varphi(g) = \psi(gK)$. $\square$

This completes the proof of Theorem 1. $\square$

There are two more Isomorphism Theorems. The second one says the product of a subgroup H and a normal subgroup N is a subgroup, and $(HN)/N \cong H/(H \cap N)$. The third one says if H is a subgroup in G that contains a normal subgroup N, then $(G/N)/(H/N) \cong G/K$.

Example: Special Linear Group

Example 1

Recall part (**??**) of Example **??**, the group homomorphism

$$\begin{aligned} \delta : \mathrm{GL}(2, \mathbb{R}) &\to \mathbb{R}^\times \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto ad - bc. \end{aligned}$$

Question

What is $\ker \delta$ in Example 1?

The kernel in Example 1 is called the **special linear group** and is denoted $\mathrm{SL}(2,\mathbb{R})$. It is the set of all 2×2 matrices with real entries, whose determinant is 1. Similarly, we have $\mathrm{SL}(n,\mathbb{R})$ for each $n \in \mathbb{N}$.

Exercise 1

Prove δ in Example 1 is surjective.

It follows, from the First Isomorphism Theorem, that

$$\mathrm{GL}(2,\mathbb{R})/\,\mathrm{SL}(2,\mathbb{R}) \cong \mathbb{R}^{\times}.$$

Question

What are the cosets of $\mathrm{SL}(2,\mathbb{R})$ in $\mathrm{GL}(2,\mathbb{R})$?

Alternatively, suppose $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathsf{GL}(2, \mathbb{R})$. We can write

$$A = \begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{a}{\Delta} & \frac{b}{\Delta} \\ c & d \end{pmatrix},$$

where $\Delta = \det A \neq 0$ and note,

$$\det \begin{pmatrix} \frac{a}{\Delta} & \frac{b}{\Delta} \\ c & d \end{pmatrix} = 1 \quad \Longrightarrow \quad \begin{pmatrix} \frac{a}{\Delta} & \frac{b}{\Delta} \\ c & d \end{pmatrix} \in \mathsf{SL}(2, \mathbb{R}).$$

So A is in the coset $\left(\begin{smallmatrix} \Delta & 0 \\ 0 & 1 \end{smallmatrix}\right) \mathsf{SL}(2, \mathbb{R})$, as is any other invertible matrix with determinant Δ. Thus we get an isomorphism

$$\begin{gathered} \mathsf{GL}(2, \mathbb{R}) / \mathsf{SL}(2, \mathbb{R}) \xrightarrow{\cong} \mathbb{R}^{\times} \\ \begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix} \mathsf{SL}(2, \mathbb{R}) \mapsto \Delta. \end{gathered}$$

The following exercises motivate Theorem 2.

Exercise 2 (cf. Problem 74)

Use the First Isomorphism Theorem to prove $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Let us define a "basis" for the n-tuples in $\mathbb{Z}^n$. For each $i = 1, \ldots, n$, let

$$\mathbf{e}_i := (e_{i1}, e_{i2}, \ldots, e_{in}), \text{ where } e_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

We can think of each $\mathbf{e}_i$ is a "component-wise identity" of $\mathbb{Z}^n$.

Exercise 3 (cf. Problem 75)

Let m, n denote non-zero integers. Use the First Isomorphism Theorem to show

$$\mathbb{Z}^2/\langle m\mathbf{e}_1, n\mathbf{e}_2\rangle \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

Question

How does Exercise 3 compare to Example **??**? What about Proposition **??**?

Theorem 2 is the generalization:

Theorem 2

Let $H = \langle m_1\mathbf{e}_1, \dots, m_n\mathbf{e}_n \rangle < \mathbb{Z}^n$*. Then*

$$\mathbb{Z}^n/H \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}.$$

$\square$

Proposition 1

Every finitely generated abelian group is a quotient group of $\mathbb{Z}^m$, for some $m \in \mathbb{N}$.

Proof.

Suppose G is an abelian group with generators $g_1, \ldots, g_m$. Then every element in G is of the form $g_1^{a_1} \cdots g_m^{a_m}$ for integers $a_1, \ldots, a_m$. Define a map

$$\phi : \mathbb{Z}^m \to G$$
$$\mathbf{a} := (a_1, \ldots, a_m) \mapsto g_1^{a_1} \cdots g_m^{a_m}.$$

If ϕ is surjective then we may apply the First Isomorphism Theorem to conclude

$$\mathbb{Z}^m / \ker(\phi) \cong \phi(\mathbb{Z}^m) = G,$$

completing the proof.

First we show ϕ is a group homomorphism. Suppose $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^m$.

$$\begin{aligned}
\phi(\mathbf{a}+\mathbf{b}) &= \phi\left((a_1+b_1, \ldots, a_m+b_m)\right) \\
&= g_1^{a_1+b_1} \cdots g_n^{a_m+b_m} \\
&= (g_1^{a_1} g_1^{b_1}) \cdots (g_m^{a_m} g_m^{b_m}) \\
&= (g_1^{a_1} \cdots g_m^{a_m})(g_1^{b_1} \cdots g_m^{b_m}) \\
&= \phi\left((a_1, \ldots, a_m)\right) \phi\left(b_1, \ldots, b_m)\right).
\end{aligned}$$

Now we show ϕ is surjective. Take $g \in G$, which again, can be written $g = g_1^{a_1} \cdots g_m^{a_m}$ for some $a_1, \ldots, a_m \in \mathbb{Z}$. By definition, $\phi : (a_1, \ldots, a_m) \mapsto g$. So ϕ is surjective. $\square$

The **Fundamental Theorem of Finitely Generated Abelian Groups**, which we state in Section **??**, actually gives the precise structure of the quotient groups in Proposition 1.

Solutions to exercises

Exercise 1

Solution: Suppose $x \in \mathbb{R}^+$. The matrix $X = \left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is in $\mathrm{GL}(2, \mathbb{R})$ and has determinant equal to x. So $\delta(X) = x$. $\square$

Exercise 2 (cf. Problem 74)

Solution: Define $\bar{\varphi} : \mathbb{Z} \to \mathbb{Z}_n$ by mapping $a \in \mathbb{Z}$ to $a \pmod{n}$. Then $\bar{\varphi}$ is surjective, and the kernel consists of multiples of n, i.e., the subgroup $n\mathbb{Z}$. By the First Isomorphism Theorm, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. $\square$

Exercise 3 (cf. Problem 75)

Solution: We define a map on the generators of $\mathbb{Z}^2$:

$$\begin{aligned} \bar{\varphi} : \mathbb{Z}^2/ &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ \mathbf{e}_1 &\mapsto (1, 0) \\ \mathbf{e}_2 &\mapsto (0, 1) \end{aligned}$$

Then $(a, b) \in \mathbb{Z}^2$ maps to $(a \pmod{n}, b \pmod{n})$ and so $\bar{\varphi}$ is surjective. The kernel is generated by $m\mathbf{e}_1$ and $n\mathbf{e}_2$. Therefore the First Isomorphism Theorem syas $\mathbb{Z}^2/\langle m\mathbf{e}_1, n\mathbf{e}_2\rangle \cong \mathbb{Z}_m \times \mathbb{Z}_n$. $\square$