Math 3230 Abstract Algebra I
Sec 4.3: The fundamental homomorphism theorem

Slides created by M. Macauley, Clemson (Modified by E. Gunawan, UConn)

http://egunawan.github.io/algebra

Abstract Algebra I

Quotients: via Cayley diagrams

Recall $Q_8 = \{\pm 1, \pm i, \pm i, \pm k\}$ with $ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$.

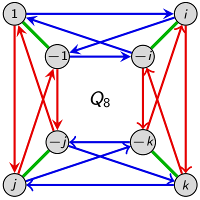
Define the homomorphism $\phi : Q_8 \to V_4$ via $\phi(i) = v$ and $\phi(j) = h$. Since $Q_8 = \langle i, j \rangle$, we can determine where ϕ sends the remaining elements:

$$\phi(1) = e\,, \qquad \phi(-1) = \phi(i^2) = \phi(i)^2 = v^2 = e\,,$$

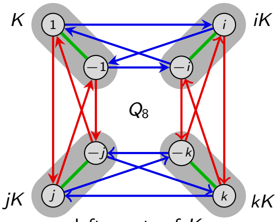
$$\phi(k) = \phi(ij) = \phi(i)\phi(j) = vh = r\,, \qquad \phi(-k) = \phi(ji) = \phi(j)\phi(i) = hv = r\,,$$

$$\phi(-i) = \phi(-1)\phi(i) = ev = v\,, \qquad \phi(-j) = \phi(-1)\phi(j) = eh = h\,.$$

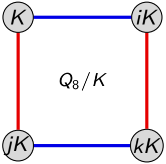
Note that $\operatorname{Ker}\phi = \{-1, 1\}$. Let's see what happens when we quotient out by $\operatorname{Ker}\phi$:



Q_8 organized by the subgroup $K = \langle -1 \rangle$



left cosets of K are near each other



collapse cosets into single nodes

Do you notice any relationship between $Q_8/\operatorname{Ker}(\phi)$ and $\operatorname{Im}(\phi)$?

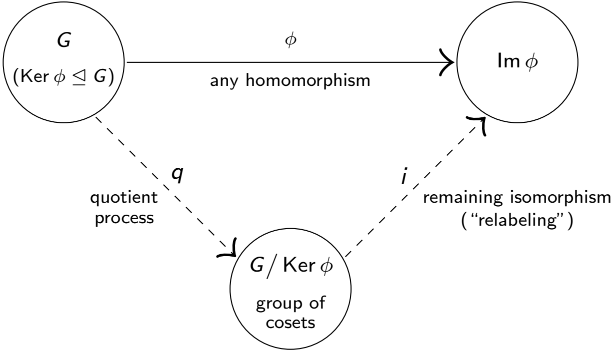
The Fundamental Homomorphism Theorem

The following is one of the central results in group theory.

Fundamental homomorphism theorem (FHT)

If $\phi\colon G \to H$ is a homomorphism, then $\mathrm{Im}(\phi) \cong G/\operatorname{Ker}(\phi)$.

The FHT says that every homomorphism can be decomposed into two steps: (i) quotient out by the kernel, and then (ii) relabel the nodes via ϕ.



Proof of the FHT

Fundamental homomorphism theorem

If $\phi\colon G \to H$ is a homomorphism, then $\mathrm{Im}(\phi) \cong G/\,\mathrm{Ker}(\phi)$.

Proof

We will construct an explicit map $i\colon G/\,\mathrm{Ker}(\phi) \longrightarrow \mathrm{Im}(\phi)$ and prove that it is an isomorphism.

Let $K := \mathrm{Ker}(\phi)$, and recall that $G/K := \{aK\colon a \in G\}$. Define

$$i\colon G/K \longrightarrow \mathrm{Im}(\phi)\,, \qquad i\colon gK \longmapsto \phi(g)\,.$$

• <u>*Show i is well-defined*</u>: We must show that if $aK = bK$, then $i(aK) = i(bK)$.

Suppose $aK = bK$. We have

$$aK = bK \quad\Longrightarrow\quad b^{-1}aK = K \quad\Longrightarrow\quad b^{-1}a \in K\,.$$

By definition of $b^{-1}a \in \mathrm{Ker}(\phi)$,

$$1_H = \phi(b^{-1}a) = \phi(b^{-1})\,\phi(a) = \phi(b)^{-1}\,\phi(a) \quad\Longrightarrow\quad \phi(a) = \phi(b)\,.$$

By definition of i: $\quad i(aK) = \phi(a) = \phi(b) = i(bK)$. ✓

Proof of FHT (cont.) [Recall: $i\colon G/K \to \mathrm{Im}(\phi)$, $i\colon gK \mapsto \phi(g)$]

Proof (cont.)

- *Show i is a homomorphism*: We must show that $i(aK \cdot bK) = i(aK)\, i(bK)$.

$$\begin{aligned} i(aK \cdot bK) &= i(abK) && (aK \cdot bK := abK \text{ from Slides 3.5 ``quotient groups''}) \\ &= \phi(ab) && (\text{definition of } i) \\ &= \phi(a)\,\phi(b) && (\phi \text{ is a homomorphism}) \\ &= i(aK)\, i(bK) && (\text{definition of } i) \end{aligned}$$

Thus, i is a homomorphism. ✓

- *Show i is surjective (onto)*:

This means showing that for any element in the codomain (here, $\mathrm{Im}(\phi)$), that some element in the domain (here, G/K) gets mapped to it by i.

Pick any $\phi(a) \in \mathrm{Im}(\phi)$. By defintion, $i(aK) = \phi(a)$, hence i is surjective. ✓

Proof of FHT (cont.) [Recall: $i\colon G/K \to \mathrm{Im}(\phi)$, $i\colon gK \mapsto \phi(g)$]

Proof (cont.)

- *Show i is injective (1–1)*: We must show that $i(aK) = i(bK)$ implies $aK = bK$.

Suppose that $i(aK) = i(bK)$. Then

$$\begin{aligned}
i(aK) = i(bK) &\implies \phi(a) = \phi(b) && \text{(by definition of the map } i\text{)} \\
&\implies \phi(b)^{-1}\,\phi(a) = 1_H && \\
&\implies \phi(b^{-1}a) = 1_H && (\phi \text{ is a homom.}) \\
&\implies b^{-1}a \in K && (\text{definition of } \mathrm{Ker}(\phi)) \\
&\implies b^{-1}aK = K && (aH = H \;\Leftrightarrow\; a \in H) \\
&\implies aK = bK &&
\end{aligned}$$

Thus, i is injective. ✓

In summary, since $i\colon G/K \to \mathrm{Im}(\phi)$ is a well-defined homomorphism that is injective (1–1) and surjective (onto), it is an **isomorphism**.

Therefore, $G/K \cong \mathrm{Im}(\phi)$, and the FHT is proven. □

Consequences of the FHT

An alternative proof of Prop 1 part 3

If $\phi\colon G \to H$ is a homomorphism, then $\operatorname{Im}\phi < H$.

A few special cases

- If $\phi\colon G \to H$ is an embedding, then $\operatorname{Ker}(\phi) = \{1_G\}$. The FHT says that
$$\operatorname{Im}(\phi) \cong G/\{1_G\} \cong G\,.$$
- If $\phi\colon G \to H$ is the map $\phi(g) = 1_H$ for all $h \in G$, then $\operatorname{Ker}(\phi) = G$, so the FHT says that
$$\{1_H\} = \operatorname{Im}(\phi) \cong G/G\,.$$

Let's use the FHT to determine all homomorphisms $\phi\colon C_4 \to C_3$:

- By the FHT, $G/\operatorname{Ker}\phi \cong \operatorname{Im}\phi < C_3$, and so $|\operatorname{Im}\phi| = 1$ or 3.
- Since $\operatorname{Ker}\phi < C_4$, Lagrange's Theorem also tells us that $|\operatorname{Ker}\phi| \in \{1,2,4\}$, and hence $|\operatorname{Im}\phi| = |G/\operatorname{Ker}\phi| \in \{1,2,4\}$.

Thus, $|\operatorname{Im}\phi| = 1$, and so the *only* homomorphism $\phi\colon C_4 \to C_3$ is the trivial one.

What does "well-defined" really mean?

Recall that we've seen the term "**well-defined**" arise in different contexts:

- a well-defined binary operation on a set G/N of cosets,
- a well-defined function $i\colon G/N \to H$ from a set (group) of cosets.

In both of these cases, well-defined means that:

our definition doesn't depend on our choice of coset representative.

Formally:

- If $N \trianglelefteq G$, then $aN \cdot bN := abN$ is a well-defined binary operation on the set G/N of cosets, because

$$\text{if } a_1N = a_2N \text{ and } b_1N = b_2N, \text{ then } a_1b_1N = a_2b_2N.$$

- The map $i\colon G/K \to H$, where $i(aK) = \phi(a)$, is a well-defined homomorphism, meaning that

$$\text{if } aK = bK, \text{ then } i(aK) = i(bK) \text{ (that is, } \phi(a) = \phi(b)\text{) holds.}$$

Whenever we define a map and the domain is a *quotient*, we must show it's well-defined.

How to show two groups are isomorphic

The standard way to show $G \cong H$ is to construct an isomorphism $\phi \colon G \to H$.

When the domain is a quotient, there is another method, due to the FHT.

Useful technique

Suppose we want to show that $G/N \cong H$. There are two approaches:

(i) Define a map $\phi \colon G/N \to H$ and prove that it is well-defined, a homomorphism, and a bijection.

(ii) Define a map $\phi \colon G \to H$ and prove that it is a homomorphism, a surjection (onto), and that $\operatorname{Ker} \phi = N$.

Usually, Method (ii) is easier. Showing well-definedness and injectivity can be tricky.

For example, each of the following are results for which (ii) works quite well:

- $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$;
- $\mathbb{Q}^*/\langle -1 \rangle \cong \mathbb{Q}^+$;
- $AB/B \cong A/(A \cap B)$ (assuming $A, B \trianglelefteq G$);
- $G/(A \cap B) \cong (G/A) \times (G/B)$ (assuming $G = AB$).

Cyclic groups as quotients

Consider the following (normal) subgroup of $\mathbb{Z}$:

$$12\mathbb{Z} = \langle 12 \rangle = \{\dots, -24, -12, 0, 12, 24, \dots\} \lhd \mathbb{Z}\,.$$

The *elements* of the quotient group $\mathbb{Z}/\langle 12 \rangle$ are the *cosets*:

$$0 + \langle 12 \rangle\,, \quad 1 + \langle 12 \rangle\,, \quad 2 + \langle 12 \rangle \quad, \ \dots\ , \quad 10 + \langle 12 \rangle\,, \quad 11 + \langle 12 \rangle\,.$$

Number theorists call these sets congruence classes modulo 12. We say that two numbers are congruent mod 12 if they are in the same coset.

Recall how to add cosets in the quotient group:

$$(a + \langle 12 \rangle) + (b + \langle 12 \rangle) := (a + b) + \langle 12 \rangle\,.$$

"(The coset containing a) + (the coset containing b) = the coset containing $a + b$."

It should be clear that $\mathbb{Z}/\langle 12 \rangle$ is isomorphic to $\mathbb{Z}_{12}$. Formally, this is just the FHT applied to the following homomorphism:

$$\phi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_{12}\,, \qquad \phi\colon k \longmapsto k \pmod{12}\,,$$

Clearly, $\mathrm{Ker}(\phi) = \{\dots, -24, -12, 0, 12, 24, \dots\} = \langle 12 \rangle$. By the FHT:

$$\mathbb{Z}/\operatorname{Ker}(\phi) = \mathbb{Z}/\langle 12 \rangle \cong \operatorname{Im}(\phi) = \mathbb{Z}_{12}\,.$$

A picture of the isomorphism $i\colon \mathbb{Z}_{12} \longrightarrow \mathbb{Z}/\langle 12\rangle$ (from the VGT website)