Homomorphisms

Course Title: Advanced Cryptography
Course Code: ICT-6115

Mawlana Bhashani
Science and Technology University

Presented By:

Md. Shamsuzzaman Miah
IT-23624
Department of ICT, MBSTU

Presented To:

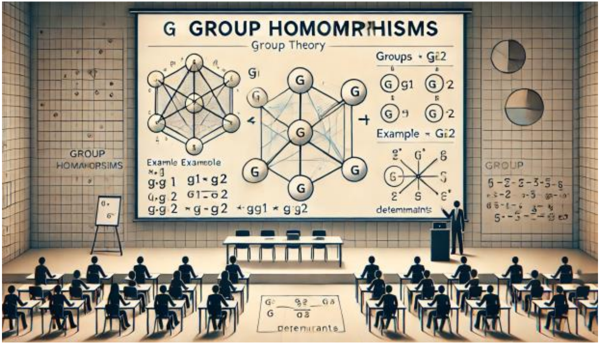
Mr. Ziaur Rahman
Associate Professor
Dept. of ICT,MBSTU

Group Homomorphisms

A homomorphism between groups (G, ·) and (H, ∘) is a map $\phi : G \rightarrow H$ such that

$$\phi(g1 \cdot g2) = \phi(g1) \circ \phi(g2)$$

for g1, g2 ∈ G. The range of ϕ in H is called the homomorphic image of ϕ



Homomorphisms

Throughout the course, we've said things like:

- "This group has the same structure as that group."
- "This group is isomorphic to that group."

We will study a special type of function between groups, called a *homomorphism*. An *isomorphism* is a homomorphism which is a bijection.

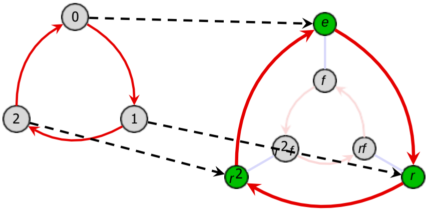
There are two situations where homomorphisms arise:

- when one group is a subgroup of another;
- when one group is a quotient of another.

The corresponding homomorphisms are called embeddings and quotient maps.

Example

Consider the statement: $Z_3 < D_3$. Here is a visual:



$0 \mapsto e$

$1 \mapsto r$

$2 \mapsto r^2$

The group D_3 contains a size-3 cyclic subgroup $\langle r \rangle$, which is identical to Z_3 in structure only. None of the elements of Z_3 (namely 0, 1, 2) are actually in D_3.

When we say $Z_3 < D_3$, we really mean that the structure of Z_3 shows up in D_3.

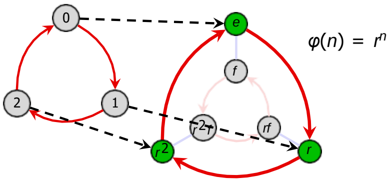
In particular, there is a bijective correspondence between the elements in Z_3 and those in the subgroup $\langle r \rangle$ in D_3. Furthermore, the *relationship* between the corresponding nodes is the same.

A homomorphism is the mathematical tool for succinctly expressing precise structural correspondences. It is a *function* between groups satisfying a few "natural" properties.

Homomorphisms

Using the previous example, we say that this function maps elements of $\mathbb{Z}_3$ to elements of D_3. We may write this as

$$\varphi \colon \mathbb{Z}_3 \dashrightarrow D_3 \, .$$



The group *from* which a function originates is the domain ($\mathbb{Z}_3$ in our example). The group *into* which the function maps is the codomain (D_3 in our example).

The elements in the codomain that the function maps to are called the image of the function ($\{e, r, r^2\}$ in our example), denoted $\mathrm{Im}(\varphi)$. That is,

$$\mathrm{Im}(\varphi) = \varphi(G) = \{\varphi(g) \mid g \in G\} \, .$$

Definition

A homomorphism is a function $\varphi \colon (G, *) \to (H, \circ)$ between two groups satisfying

$$\varphi(a * b) = \varphi(a) \circ \varphi(b), \qquad \text{for all } a, b \in G \, .$$

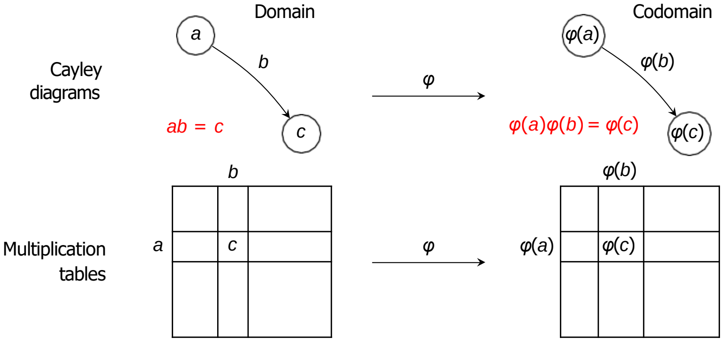
Note that the operation $a * b$ is occurring in the domain G while $\varphi(a) \circ \varphi(b)$ occurs in the codomain H.

Homomorphisms

Remark

Not every function from one group to another is a homomorphism! The condition $\varphi(a * b) = \varphi(a) \circ \varphi(b)$ preserves the structure of G.

The $\varphi(a * b) = \varphi(a) \circ \varphi(b)$ condition has visual interpretations on the level of Cayley diagrams and multiplication tables.



Note that in the Cayley diagrams, b and $\varphi(b)$ are paths; they need not just be edges.

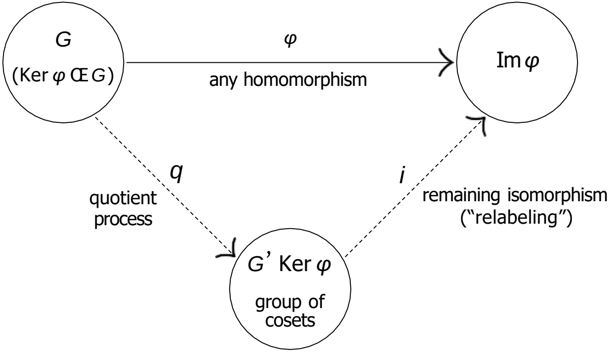
The Fundamental Homomorphism Theorem

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

Fundamental homomorphism theorem (FHT)

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

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

Proof

We will construct an explicit map $i : G/\mathrm{Ker}(\varphi) \dashrightarrow \mathrm{Im}(\varphi)$ and prove that it is an isomorphism.

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

$$i : G/K \dashrightarrow \mathrm{Im}(\varphi), \qquad i : gK \dashrightarrow \varphi(g).$$

- *Show i is well-defined*: 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 $b^{-1}a \in \mathrm{Ker}(\varphi)$,

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

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

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

Proof (cont.)

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

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

Thus, i is a homomorphism. C

- *Show i is surjective (onto)* :

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

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

Consequences of the FHT

An alternative proof of Prop 1 part 3

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

A few special cases

- If $\varphi\colon G \to H$ is an embedding, then $\operatorname{Ker}(\varphi) = \{1_G\}$. The FHT says that

$$\operatorname{Im}(\varphi) \cong G/\{1_G\} \cong G .$$

- If $\varphi\colon G \to H$ is the map $\varphi(g) = 1_H$ for all $h \in G$, then $\operatorname{Ker}(\varphi) = G$, so the FHT says that

$$\{1_H\} = \operatorname{Im}(\varphi) \cong G/G .$$

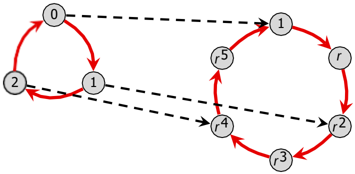
Let's use the FHT to determine all homomorphisms $\varphi\colon C_4 \to C_3$:

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

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

Types of homomorphisms

Example 3: Consider the following homomorphism $\vartheta\colon \mathbb{Z}_3 \to C_6$, defined by $\vartheta(n) = r^{2n}$:



$0 \mapsto 1$

$1 \mapsto r^2$

$2 \mapsto r^4$

It is easy to check that $\vartheta(a + b) = \vartheta(a)\vartheta(b)$: The red-arrow in $\mathbb{Z}_3$ (representing 1) gets mapped to the 2-step path representing r^2 in C_6.

A homomorphism $\varphi\colon G \to H$ that is one-to-one or "injective" is called an embedding: the group G "embeds" into H as a subgroup.

If $\varphi(G) = H$, then φ is onto, or surjective.

Definition

A homomorphism that is both injective and surjective is an **isomorphism**.

An **automorphism** is an isomorphism from a group *to itself*.

Homomorphisms and generators

Remark 1

If we know where a homomorphism maps the generators of G, we can determine where it maps *all* elements of G.

For example, suppose $\varphi : Z_3 \to Z_6$ was a homomorphism, with $\varphi(1) = 4$. Using this information, we can construct the rest of φ:

$$\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 4 + 4 = 2$$

$$\varphi(0) = \varphi(1+2) = \varphi(1) + \varphi(2) = 4 + 2 = 0.$$

Example

Suppose that $G = \langle a, b \rangle$, and $\varphi : G \to H$, and we know $\varphi(a)$ and $\varphi(b)$. Using this information we can determine the image of any element in G. For example, for $g = a^3 b^2 ab$, we have

$$\varphi(g) = \varphi(aaabbab) = \varphi(a)\,\varphi(a)\,\varphi(a)\,\varphi(b)\,\varphi(b)\,\varphi(a)\,\varphi(b).$$

What do you think $\varphi(a^{-1})$ is ?

Basic properties of homomorphisms

Proposition 1

Let $\varphi\colon G \to H$ be a homomorphism. Denote the identity of G by 1_G, and the identity of H by 1_H.

(i) $\varphi(1_G) = 1_H$ "φ sends the identity to the identity"

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$ "φ sends inverses to inverses"

(iii) Suppose $J < G$. Then $\varphi(J)$ is a subgroup of H.

(iv) Suppose $I < H$. Then the preimage $\varphi^{-1}(J)$ is a subgroup of G.

Proof

(i) Observe that $\varphi(1_G)\,\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(g) = 1_H \cdot \varphi(1_G)$. Therefore, $\varphi(1_G) = 1_H$. C

(ii) Take any $g \in G$. Observe that $\varphi(g)\,\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1_G) = 1_H$. Since $\varphi(g)\varphi(g^{-1}) = 1_H$, it follows immediately that $\varphi(g^{-1}) = \varphi(g)^{-1}$. C

(iii) Show that $1_H \in \varphi(G)$, that $\varphi(J)$ is closed under the binary operation of H, and that the inverse of each element in $\varphi(J)$ is also in $\varphi(J)$.

(iv) See Prop 11.4 in Judson's textbook: abstract.ups.edu/aata/section-group-homomorphisms.html

A word of caution

A homomorphism $\varphi\colon G \to H$ is determined by the image of the generators of G, but *not* all such image will work.

Example 4: suppose we try to define a homomorphism $\varphi\colon \mathbb{Z}_3 \to \mathbb{Z}_4$ by $\varphi(1) = 1$. Then we get

$$\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 2,$$
$$\varphi(0) = \varphi(1+1+1) = \varphi(1) + \varphi(1) + \varphi(1) = 3.$$

This is *impossible*, because $\varphi(0) = 0$. (Identity is mapped to the identity.)

Example 5: That's not to say that there isn't a homomorphism $\varphi\colon \mathbb{Z}_3 \to \mathbb{Z}_4$; note that there is always the trivial homomorphism between two groups:

$$\varphi\colon G \dashrightarrow H, \qquad \varphi(g) = 1_H \quad \text{for all } g \in G.$$

Example 6

Show that there is no embedding $\varphi\colon \mathbb{Z}_n \hookrightarrow \mathbb{Z}$, for $n \geq 2$. That is, *any* such homomorphism must satisfy $\varphi(1) = 0$.

The Isomorphism Theorems

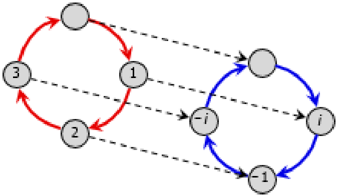
First Isomorphism Theorem: If ψ : G → H is a group homomorphism with K = ker ψ, then K is normal in G. Let φ : G → G/K be the canonical homomorphism. Then there exists a unique isomorphism η : **G/K → ψ(G) such that ψ = ηφ.**

Second Isomorphism Theorem: Let H be a subgroup of a group G (not necessarily normal in G) and N a normal subgroup of G. Then HN is a subgroup of G, H ∩ N is a normal subgroup of H, and **H/H ∩ N ∼= HN/N**

Correspondence Theorem: Let N be a normal subgroup of a group G. Then H 7→ H/N is a one-to-one correspondence between the set of subgroups H of G containing N and the set of subgroups of G/N. Furthermore, the normal subgroups of G containing N correspond to normal subgroups of G/N.

Third Isomorphism Theorem: Let G be a group and N and H be normal subgroups of G with N ⊂ H. Then

G/H ∼= (G/N) / (H/N)

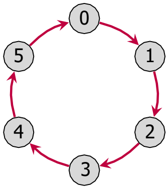


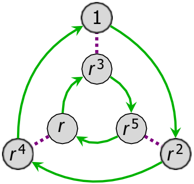
Isomorphisms

Sometimes, the isomorphism is less visually obvious because the Cayley graphs have different structure.

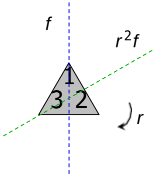
For example, the following is an isomorphism:

$$\varphi : \mathbb{Z}_6 \dashrightarrow C_6$$
$$\varphi(k) = r^k$$

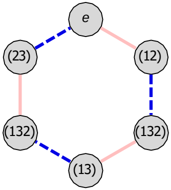


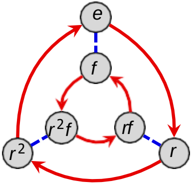


Here is another non-obvious isomorphism between $S_3 = \langle (12), (23) \rangle$ and $D_3 = \langle r, f \rangle$.



$$\varphi : S_3 \dashrightarrow D_3$$
$$\varphi : (12) \dashrightarrow r^2f$$
$$\varphi : (23) \dashrightarrow f$$





How to show two groups are isomorphic

The standard way to show $G \cong H$ is to construct an isomorphism $\varphi : G \to H$.

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 $\varphi : G/N \to H$ and prove that it is well-defined, a homomorphism, and a bijection.

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

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 $\mathbb{Z}$:

$$12\mathbb{Z} = \langle 12 \rangle = \{\ldots, -24, -12, 0, 12, 24, \ldots\} \trianglelefteq \mathbb{Z}.$$

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

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

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 $a + b$."

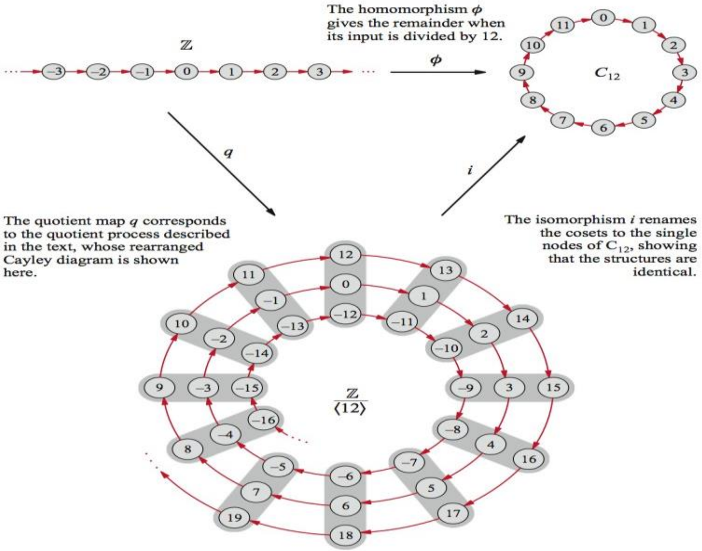
It should be clear that $\mathbb{Z}/\langle 12 \rangle$ is isomorphic to $\mathbb{Z}_{12}$. Formally, this is just the FHT applied to the following homomorphism:

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

Clearly, $\text{Ker}(\varphi) = \{\ldots, -24, -12, 0, 12, 24, \ldots\} = \langle 12 \rangle$. By the FHT:

$$\mathbb{Z}/\text{Ker}(\varphi) = \mathbb{Z}/\langle 12 \rangle \cong \text{Im}(\varphi) = \mathbb{Z}_{12}.$$

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



References

[1] **Book:** Abstract Algebra Theory and Applications by Thomas W. Judson, Stephen F. Austin State University

[2] **Website:** abstract.pugetsound.edu

[3] **Website:** https://www.math.clemson.edu/~macaule/classes/m20_math4120/slides/math4120_lecture-4-01_h.pdf

[4] **Website:** https://people.math.sc.edu/shaoyun/math5462slide9.pdf

[5] **Website:** https://egunawan.github.io/algebra/slides/sec4p3.pdf

[6] **Website:** https://tseppelt.github.io/assets/pdf/slides/20220707_slides_icalp.pdf

[7] **Website:** https://users.metu.edu.tr/matmah/2014-463/463.pdf

Any Question

Thank you!