Section 4: Maps between groups

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

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."

However, we've never really spelled out the details about what this means.

We will study a special type of function between groups, called a *homomorphism*. An *isomorphism* is a special type of homomorphism. The Greek roots "homo" and "morph" together mean "same shape."

There are two situations where homomorphisms arise:

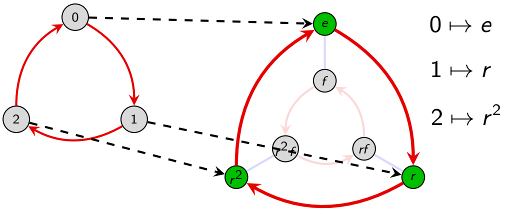
- when one group is a subgroup of another;
- when one group is a quotient of another.

The corresponding homomorphisms are called embeddings and quotient maps.

Also in this chapter, we will completely classify all finite abelian groups, and get a taste of a few more advanced topics, such as the the four "isomorphism theorems," commutator subgroups, and automorphisms.

A motivating example

Consider the statement: $\mathbb{Z}_3 < D_3$. Here is a visual:



The group D_3 contains a size-3 cyclic subgroup $\langle r \rangle$, which is identical to $\mathbb{Z}_3$ in structure only. None of the elements of $\mathbb{Z}_3$ (namely 0, 1, 2) are actually in D_3.

When we say $\mathbb{Z}_3 < D_3$, we really mean that the structure of $\mathbb{Z}_3$ shows up in D_3.

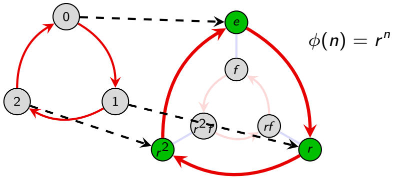
In particular, there is a bijective correspondence between the elements in $\mathbb{Z}_3$ and those in the subgroup $\langle r \rangle$ in D_3. Furthermore, the *relationship* between the corresponding nodes is the same.

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

$$\phi\colon \mathbb{Z}_3 \longrightarrow D_3 \,.$$



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 $\mathrm{Im}(\phi)$. That is,

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

Definition

A homomorphism is a function $\phi\colon G \to H$ between two groups satisfying

$$\phi(ab) = \phi(a)\phi(b), \qquad \text{for all } a, b \in G \,.$$

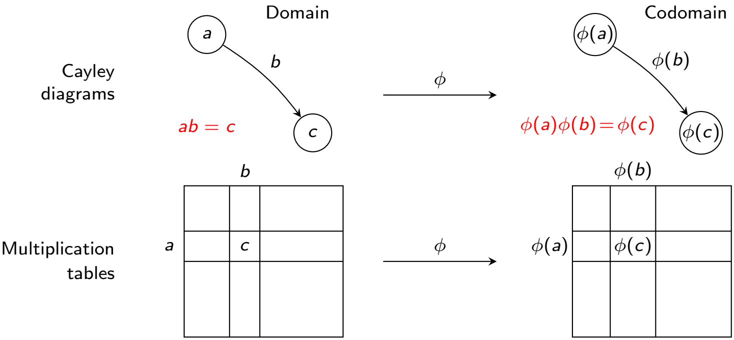
Note that the operation $a \cdot b$ is occurring in the domain while $\phi(a) \cdot \phi(b)$ occurs in the codomain.

Homomorphisms

Remark

Not every function from one group to another is a homomorphism! The condition $\phi(ab) = \phi(a)\phi(b)$ means that the map ϕ preserves the structure of G.

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



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

An example

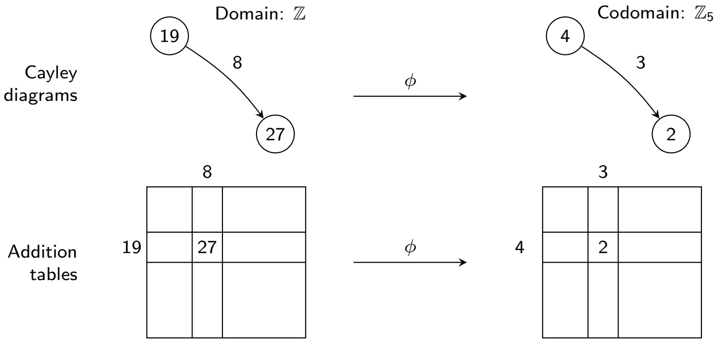
Consider the function ϕ that reduces an integer modulo 5:

$$\phi \colon \mathbb{Z} \longrightarrow \mathbb{Z}_5 , \qquad \phi(n) = n \pmod 5.$$

Since the group operation is additive, the "homomorphism property" becomes

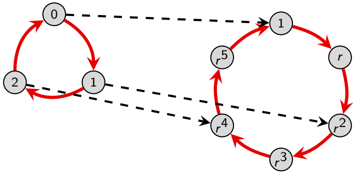
$$\phi(a+b) = \phi(a) + \phi(b) .$$

In plain English, this just says that one can "first add and then reduce modulo 5," OR "first reduce modulo 5 and then add."



Types of homomorphisms

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



$0 \mapsto 1$

$1 \mapsto r^2$

$2 \mapsto r^4$

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

A homomorphism $\phi \colon G \to H$ that is one-to-one or "injective" is called an embedding: the group G "embeds" into H as a subgroup. If θ is not one-to-one, then it is a quotient.

If $\phi(G) = H$, 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

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

For example, suppose $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6$ was a homomorphism, with $\phi(1) = 4$. Using this information, we can construct the rest of ϕ:

$$\begin{aligned}\phi(2) &= \phi(1+1) = \phi(1) + \phi(1) = 4 + 4 = 2\\ \phi(0) &= \phi(1+2) = \phi(1) + \phi(2) = 4 + 2 = 0.\end{aligned}$$

Example

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

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

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

Two basic properties of homomorphisms

Proposition

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

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

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

Proof

(i) Pick any $g \in G$. Now, $\phi(g) \in H$; observe that

$$\phi(1_G)\,\phi(g) = \phi(1_G \cdot g) = \phi(g) = 1_H \cdot \phi(g)\,.$$

Therefore, $\phi(1_G) = 1_H$. ✓

(ii) Take any $g \in G$. Observe that

$$\phi(g)\,\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1_G) = 1_H\,.$$

Since $\phi(g)\phi(g^{-1}) = 1_H$, it follows immediately that $\phi(g^{-1}) = \phi(g)^{-1}$. ✓ □

A word of caution

Just because a homomorphism $\phi\colon G \to H$ is determined by the image of its generators does *not* mean that every such image will work.

For example, suppose we try to define a homomorphism $\phi\colon \mathbb{Z}_3 \to \mathbb{Z}_4$ by $\phi(1) = 1$. Then we get

$$\begin{aligned} \phi(2) &= \phi(1+1) = \phi(1) + \phi(1) = 2, \\ \phi(0) &= \phi(1+1+1) = \phi(1) + \phi(1) + \phi(1) = 3\,. \end{aligned}$$

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

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

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

Exercise

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

Isomorphisms

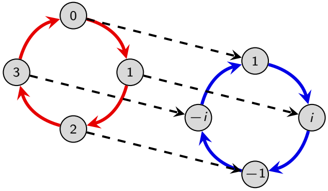
Two isomorphic groups may name their elements differently and may look different based on the layouts or choice of generators for their Cayley diagrams, but the isomorphism between them guarantees that they have the same structure.

When two groups G and H have an isomorphism between them, we say that G and H are isomorphic, and write $G \cong H$.

The roots of the polynomial $f(x) = x^4 - 1$ are called the 4th roots of unity, and denoted $R(4) := \{1, i, -1, -i\}$. They are a subgroup of $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$, the nonzero complex numbers under multiplication.

The following map is an isomorphism between $\mathbb{Z}_4$ and $R(4)$.

$$\phi \colon \mathbb{Z}_4 \longrightarrow R(4)\,, \qquad \phi(k) = i^k\,.$$

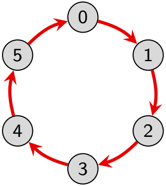


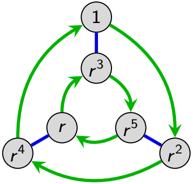
Isomorphisms

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

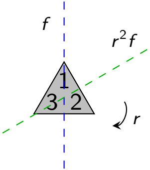
For example, the following is an isomorphism:

$$\phi \colon \mathbb{Z}_6 \longrightarrow C_6$$
$$\phi(k) = r^k$$

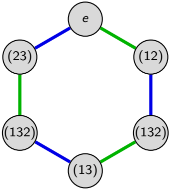


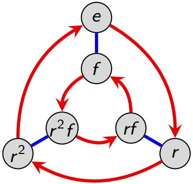


Here is another non-obvious isomorphism between $S_3 = \langle (12), (23) \rangle$ and $D_3 = \langle r, f \rangle$.



$$\phi \colon S_3 \longrightarrow D_3$$
$$\phi \colon (12) \longmapsto r^2 f$$
$$\phi \colon (23) \longmapsto f$$





Another example: the quaternions

Let $\mathrm{GL}_n(\mathbb{R})$ be the set of invertible $n \times n$ matrices with real-valued entries. It is easy to see that this is a group under multiplication.

Recall the quaternion group $Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = -1,\ ij = k \rangle$.

The following set of 8 matrices forms an isomorphic group under multiplication, where I is the 4×4 identity matrix:

$$\left\{ \pm I, \quad \pm \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \pm \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad \pm \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \right\}.$$

Formally, we have an embedding $\phi\colon Q_8 \to \mathrm{GL}_4(\mathbb{R})$ where

$$\phi(i) = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \phi(j) = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad \phi(k) = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

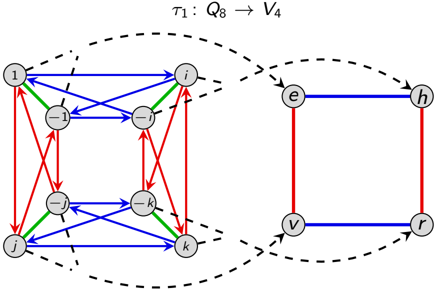
We say that Q_8 is represented by a set of matrices.

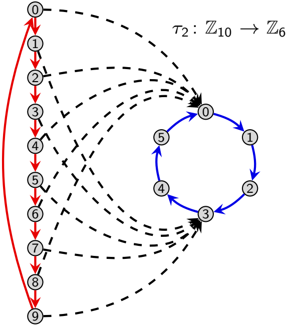
Many other groups can be represented by matrices. Can you think of how to represent V_4, C_n, or S_n, using matrices?

Quotient maps

Consider a homomorphism where more than one element of the domain maps to the same element of the codomain (i.e., non-embeddings).

Here are some examples.





Non-embedding homomorphisms are called quotient maps (as we'll see, they correspond to our quotient process).

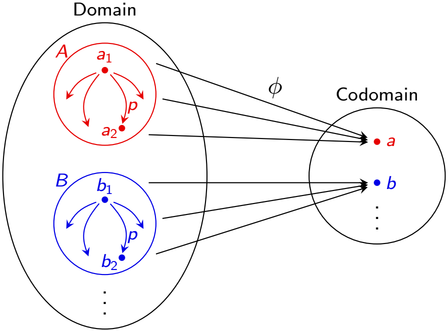
Preimages

Definition

If $\phi\colon G \to H$ is a homomorphism and $h \in \operatorname{Im}(\phi) < H$, define the preimage of h to be the set

$$\phi^{-1}(h) := \{g \in G : \phi(g) = h\}.$$

Observe in the previous examples that the preimages all had the same structure. This always happens.



The preimage of $1_H \in H$ is called the kernel of ϕ, denoted $\operatorname{Ker}\phi$.

Preimages

Observation 1

All preimages of ϕ have the same structure.

Proof (sketch)

Pick two elements $a, b \in \phi(G)$, and let $A = \phi^{-1}(a)$ and $B = \phi^{-1}(b)$ be their preimages.

Consider any path $a_1 \xrightarrow{p} a_2$ between elements in A. For any $b_1 \in B$, there is a corresponding path $b_1 \xrightarrow{p} b_2$. *We need to show that $b_2 \in B$.*

Since homomorphisms preserve structure, $\phi(a_1) \xrightarrow{\phi(p)} \phi(a_2)$. Since $\phi(a_1) = \phi(a_2)$, $\phi(p)$ is the *trivial path*.

Therefore, $\phi(b_1) \xrightarrow{\phi(p)} \phi(b_2)$, i.e., $\phi(b_1) = \phi(b_2)$, and so by definition, $b_2 \in B$. $\square$

Clearly, G is partitioned by preimages of ϕ. Additionally, we just showed that they all have the same structure. (Sound familiar?)

Preimages and kernels

Definition

The kernel of a homomorphism $\phi\colon G \to H$ is the set

$$\operatorname{Ker}(\phi) := \phi^{-1}(e) = \{k \in G : \phi(k) = e\}\,.$$

Observation 2

(i) The preimage of the identity (i.e., $K = \operatorname{Ker}(\phi)$) is a subgroup of G.

(ii) All other preimages are left cosets of K.

Proof (of (i))

Let $K = \operatorname{Ker}(\phi)$, and take $a, b \in K$. We must show that K satisfies 3 properties:

Identity: $\phi(e) = e$. $\checkmark$

Closure: $\phi(ab) = \phi(a)\,\phi(b) = e \cdot e = e$. $\checkmark$

Inverses: $\phi(a^{-1}) = \phi(a)^{-1} = e^{-1} = e$. $\checkmark$

Thus, K is a subgroup of G. $\square$

Kernels

Observation 3

Ker(ϕ) is a normal subgroup of G.

Proof

Let $K = \text{Ker}(\phi)$. We will show that if $k \in K$, then $gkg^{-1} \in K$. Take any $g \in G$, and observe that

$$\phi(gkg^{-1}) = \phi(g)\,\phi(k)\,\phi(g^{-1}) = \phi(g) \cdot e \cdot \phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e\,.$$

Therefore, $gkg^{-1} \in \text{Ker}(\phi)$, so $K \trianglelefteq G$. $\square$

Key observation

Given any homomorphism $\phi \colon G \to H$, we can *always* form the quotient group $G/\,\text{Ker}(\phi)$.

Quotients: via multiplication tables

Recall that $C_2 = \{e^{0\pi i}, e^{1\pi i}\} = \{1, -1\}$. Consider the following (quotient) homomorphism:

$$\phi\colon D_4 \longrightarrow C_2\,, \qquad \text{defined by} \quad \color{red}{\phi(r) = 1} \quad \text{and} \quad \color{green}{\phi(f) = -1}\,.$$

Note that $\phi(\text{rotation}) = 1$ and $\phi(\text{reflection}) = -1$.

The quotient process of "shrinking D_4 down to C_2" can be clearly seen from the multiplication tables.

	e	r	r^2	r^3	f	rf	r^2f	r^3f
e	e	r	r^2	r^3	f	rf	r^2f	r^3f
r	r	r^2	r^3	e	rf	r^2f	r^3f	f
r^2	r^2	r^3	e	r	r^2f	r^3f	f	rf
r^3	r^3	e	r	r^2	r^3f	f	rf	r^2f
f	f	r^3f	r^2f	rf	e	r^3	r^2	r
rf	rf	f	r^3f	r^2f	r	e	r^3	r^2
r^2f	r^2f	rf	f	r^3f	r^2	r	e	r^3
r^3f	r^3f	r^2f	rf	f	r^3	r^2	r	e

	e	r	r^2	r^3	f	rf	r^2f	r^3f
e	e	r	r^2	r^3	f	rf	r^2f	r^3f
r	r	r^2	r^3	e	rf	r^2f	r^3f	f
r^2	r^2	r^3	e	r	r^2f	r^3f	f	rf
r^3	r^3	e	r	r^2	r^3f	f	rf	r^2f
f	f	r^3f	r^2f	rf	e	r^3	r^2	r
rf	rf	f	r^3f	r^2f	r	e	r^3	r^2
r^2f	r^2f	rf	f	r^3f	r^2	r	e	r^3
r^3f	r^3f	r^2f	rf	f	r^3	r^2	r	e

non-flip **flip**

flip **non-flip**

	1	-1
1	1	-1
-1	-1	1

Quotients: via Cayley diagrams

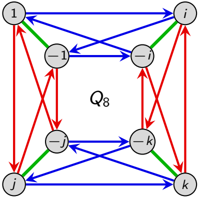
Define the homomorphism $\phi: Q_8 \to V_4$ via $\phi(i) = v$ and $\phi(j) = h$. Since $Q_8 = \langle i, j \rangle$, we can determine where ϕ sends the remaining elements:

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

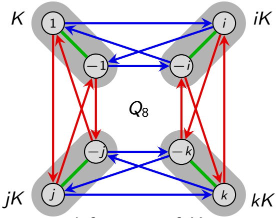
$$\phi(k) = \phi(ij) = \phi(i)\phi(j) = vh = r\,, \qquad \phi(-k) = \phi(ji) = \phi(j)\phi(i) = hv = r\,,$$

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

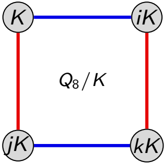
Note that $\operatorname{Ker}\phi = \{-1, 1\}$. Let's see what happens when we quotient out by $\operatorname{Ker}\phi$:



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 $\operatorname{Im}(\phi)$?

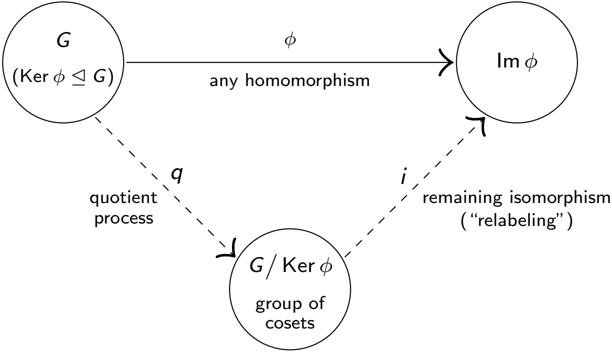
The Fundamental Homomorphism Theorem

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 $\operatorname{Im}(\phi) \cong G/\operatorname{Ker}(\phi)$.

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 $\mathrm{Im}(\phi) \cong G/\operatorname{Ker}(\phi)$.

Proof

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

Let $K = \operatorname{Ker}(\phi)$, and recall that $G/K = \{aK : a \in G\}$. 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 $b^{-1}a \in \operatorname{Ker}(\phi)$,

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

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

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

Proof (cont.)

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

$$\begin{aligned} i(aK \cdot bK) &= i(abK) && (aK \cdot bK := abK) \\ &= \phi(ab) && (\text{definition of } i) \\ &= \phi(a)\,\phi(b) && (\phi \text{ is a homomorphism}) \\ &= i(aK)\, i(bK) && (\text{definition of } i) \end{aligned}$$

Thus, i is a homomorphism. ✓

- *Show i is surjective (onto)*:

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

Pick any $\phi(a) \in \text{Im}(\phi)$. 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

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

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

Corollary

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

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

  if $a_1N = a_2N$ and $b_1N = b_2N$, 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

  if $aK = bK$, then $i(aK) = i(bK)$ (that is, $\phi(a) = \phi(b)$) 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 that we will see very soon, 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 $a + b$."

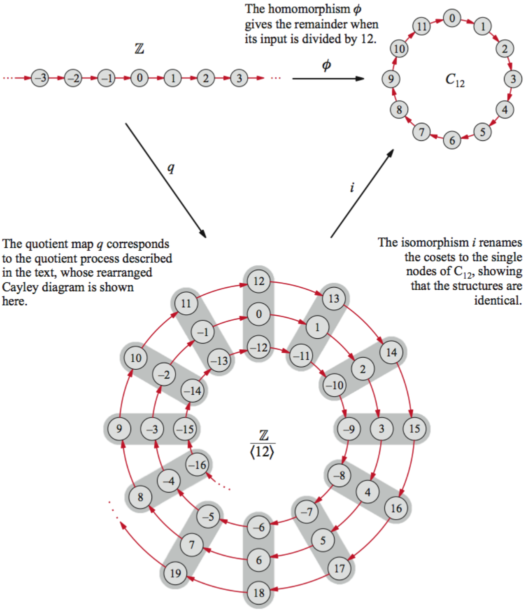
It should be clear that $\mathbb{Z}/\langle 12 \rangle$ is isomorphic to $\mathbb{Z}_{12}$. Formally, this is just the FHT applied to the following homomorphism:

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

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

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

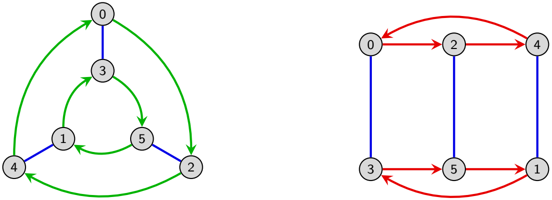
A picture of the isomorphism $i\colon \mathbb{Z}_{12} \longrightarrow \mathbb{Z}/\langle 12\rangle$ (from the VGT website)



Finite abelian groups

We've seen that some cyclic groups can be expressed as a direct product, and others cannot.

Below are two ways to lay out the Cayley diagram of $\mathbb{Z}_6$ so the direct product structure is obvious: $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$.



However, the group $\mathbb{Z}_8$ *cannot* be written as a direct product. No matter how we draw the Cayley graph, there *must* be an arrow of order 8. (Why?)

We will answer the question of when $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$, and in doing so, completely classify all finite abelian groups.

Finite abelian groups

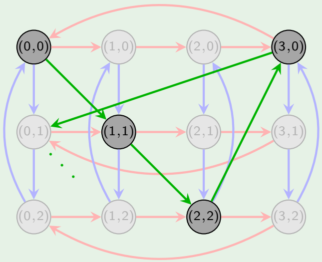
Proposition

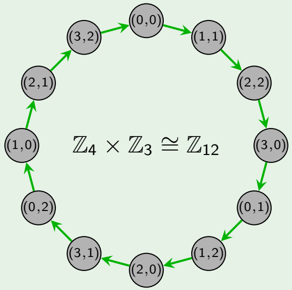
$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ if and only if $\gcd(n, m) = 1$.

Proof (sketch)

"$\Leftarrow$": Suppose $\gcd(n, m) = 1$. We claim that $(1, 1) \in \mathbb{Z}_n \times \mathbb{Z}_m$ has order nm.

$|(1, 1)|$ is the smallest k such that "$(k, k) = (0, 0)$." This happens iff $n \mid k$ and $m \mid k$. Thus, $k = \operatorname{lcm}(n, m) = nm$. ✓





Finite abelian groups

Proposition

$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ if an only if $\gcd(n, m) = 1$.

Proof (cont.)

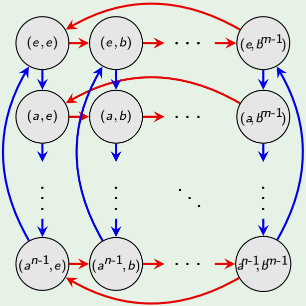
"$\Rightarrow$": Suppose $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$. Then $\mathbb{Z}_n \times \mathbb{Z}_m$ has an element (a, b) of order nm.

For convenience, we will switch to "multiplicative notation", and denote our cyclic groups by C_n.

Clearly, $\langle a \rangle = C_n$ and $\langle b \rangle = C_m$. Let's look at a Cayley diagram for $C_n \times C_m$.

The order of (a, b) must be a multiple of n (the number of rows), *and* of m (the number of columns).

By definition, this is the *least* common multiple of n and m.



But $|(a, b)| = nm$, and so $\operatorname{lcm}(n, m) = nm$. Therefore, $\gcd(n, m) = 1$. $\square$

The Fundamental Theorem of Finite Abelian Groups

Classification theorem (by "prime powers")

Every finite abelian group A is isomorphic to a direct product of cyclic groups, i.e., for some integers $n_1, n_2, \dots, n_m$,

$$A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m} ,$$

where each n_i is a prime power, i.e., $n_i = p_i^{d_i}$, where p_i is prime and $d_i \in \mathbb{N}$.

The proof of this is more advanced, and while it is at the undergraduate level, we don't yet have the tools to do it.

However, we will be more interested in understanding and utilizing this result.

Example

Up to isomorphism, there are 6 abelian groups of order $200 = 2^3 \cdot 5^2$:

$\mathbb{Z}_8 \times \mathbb{Z}_{25}$	$\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25}$	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

The Fundamental Theorem of Finite Abelian Groups

Finite abelian groups can be classified by their "elementary divisors." The mysterious terminology comes from the theory of modules (a graduate-level topic).

Classification theorem (by "elementary divisors")

Every finite abelian group A is isomorphic to a direct product of cyclic groups, i.e., for some integers $k_1, k_2, \dots, k_m$,

$$A \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_m}.$$

where each k_i is a multiple of k_{i+1}.

Example

Up to isomorphism, there are 6 abelian groups of order $200 = 2^3 \cdot 5^2$:

by "prime-powers"	by "elementary divisors"
$\mathbb{Z}_8 \times \mathbb{Z}_{25}$	$\mathbb{Z}_{200}$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$	$\mathbb{Z}_{100} \times \mathbb{Z}_2$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$	$\mathbb{Z}_{50} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
$\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_{40} \times \mathbb{Z}_5$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_{20} \times \mathbb{Z}_{10}$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$

The Fundamental Theorem of Finitely Generated Abelian Groups

Just for fun, here is the classification theorem for all *finitely generated* abelian groups. Note that it is not much different.

Theorem

Every finitely generated abelian group A is isomorphic to a direct product of cyclic groups, i.e., for some integers $n_1, n_2, \dots, n_m$,

$$A \cong \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{k \text{ copies}} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m} ,$$

where each n_i is a prime power, i.e., $n_i = p_i^{d_i}$, where p_i is prime and $d_i \in \mathbb{N}$.

In other words, A is isomorphic to a (multiplicative) group with presentation:

$$A = \langle a_1, \dots, a_k, r_1, \dots, r_m \mid r_i^{n_i} = 1,\ a_i a_j = a_j a_i,\ r_i r_j = r_j r_i,\ a_i r_j = r_j a_i \rangle .$$

In summary, (finitely generated) abelian groups are relatively easy to understand.

In contrast, nonabelian groups are more mysterious and complicated. Soon, we will study the *Sylow Theorems* which will help us better understand the structure of finite nonabelian groups.

The Isomorphism Theorems

The Fundamental Homomorphism Theorem (FHT) is the first of four basic theorems about homomorphism and their structure.

These are commonly called "The Isomorphism Theorems":

- First Isomorphism Theorem: "Fundamental Homomorphism Theorem"
- Second Isomorphism Theorem: "Diamond Isomorphism Theorem"
- Third Isomorphism Theorem: "Freshman Theorem"
- Fourth Isomorphism Theorem: "Correspondence Theorem"

All of these theorems have analogues in other algebraic structures: rings, vector spaces, modules, and Lie algebras, to name a few.

In this lecture, we will summarize the last three isomorphism theorems and provide visual pictures for each.

We will prove one, outline the proof of another (homework!), and encourage you to try the (very straightforward) proofs of the multiple parts of the last one.

Finally, we will introduce the concepts of a commutator and commutator subgroup, whose quotient yields the abelianization of a group.

The Second Isomorphism Theorem

Diamond isomorphism theorem

Let $H \leq G$, and $N \trianglelefteq G$. Then

(i) The product $HN = \{hn \mid h \in H,\ n \in N\}$ is a subgroup of G.

(ii) The intersection $H \cap N$ is a *normal* subgroup of G.

(iii) The following quotient groups are isomorphic:

$$HN/N \cong H/(H \cap N)$$

$$\begin{tikzcd}
& G \arrow[d, dash] & \\
& HN \arrow[dl, dash] \arrow[dr, dash] & \\
H \arrow[dr, dash] & & N \arrow[dl, dash] \\
& H \cap N &
\end{tikzcd}$$

Proof (sketch)

Define the following map

$$\phi \colon H \longrightarrow HN/N\,, \qquad \phi \colon h \longmapsto hN\,.$$

If we can show:

1. ϕ is a homomorphism,
2. ϕ is surjective (onto),
3. $\operatorname{Ker}\phi = H \cap N$,

then the result will follow *immediately* from the FHT. The details are left as HW.

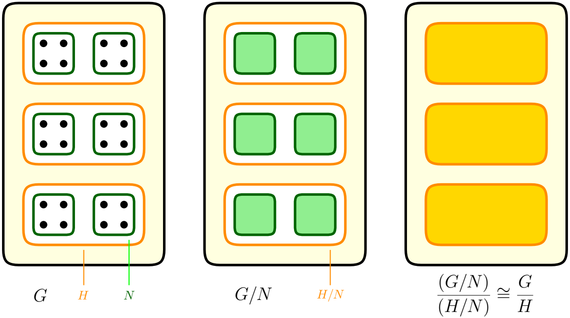
The Third Isomorphism Theorem

Freshman theorem

Consider a chain $N \leq H \leq G$ of normal subgroups of G. Then

1. The quotient H/N is a normal subgroup of G/N;
2. The following quotients are isomorphic:

$$(G/N)/(H/N) \cong G/H\,.$$



(Thanks to Zach Teitler of Boise State for the concept and graphic!)

The Third Isomorphism Theorem

Freshman theorem

Consider a chain $N \leq H \leq G$ of normal subgroups of G. Then $H/N \trianglelefteq G/N$ and $(G/N)/(H/N) \cong G/H$.

Proof

It is easy to show that $H/N \trianglelefteq G/N$ (exercise). Define the map

$$\varphi\colon G/N \longrightarrow G/H, \qquad \varphi\colon gN \longmapsto gH.$$

- *Show φ is well-defined*: Suppose $g_1N = g_2N$. Then $g_1 = g_2n$ for some $n \in N$. But $n \in H$ because $N \leq H$. Thus, $g_1H = g_2H$, i.e., $\varphi(g_1N) = \varphi(g_2N)$. ✓
- *φ is clearly onto and a homomorphism*. ✓
- *Apply the FHT*:

$$\begin{aligned} \operatorname{Ker}\varphi &= \{gN \in G/N \mid \varphi(gN) = H\} \\ &= \{gN \in G/N \mid gH = H\} \\ &= \{gN \in G/N \mid g \in H\} = H/N \end{aligned}$$

By the FHT, $(G/N)/\operatorname{Ker}\varphi = (G/N)/(H/N) \cong \operatorname{Im}\varphi = G/H$. □

The Fourth Isomorphism Theorem

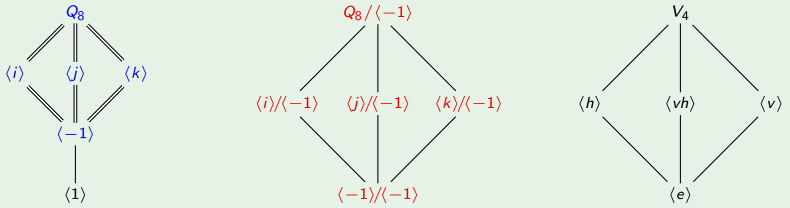
The full statement is a bit technical, so here we just state it informally.

Correspondence theorem

Let $N \trianglelefteq G$. There is a 1–1 correspondence between subgroups of G/N and subgroups of G that contain N. In particular, every subgroup of G/N has the form $\overline{A} := A/N$ for some A satisfying $N \leq A \leq G$.

This means that the corresponding subgroup lattices are identical in structure.

Example



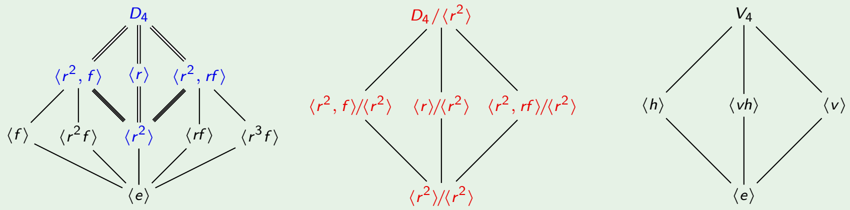
The quotient $Q_8/\langle -1 \rangle$ is isomorphic to V_4. The subgroup lattices can be visualized by "collapsing" $\langle -1 \rangle$ to the identity.

Correspondence theorem (formally)

Let $N \trianglelefteq G$. Then there is a bijection from the subgroups of G/N and subgroups of G that contain N. In particular, every subgroup of G/N has the form $\overline{A} := A/N$ for some A satisfying $N \leq A \leq G$. Moreover, if $A, B \leq G$, then

1. $A \leq B$ if and only if $\overline{A} \leq \overline{B}$,
2. If $A \leq B$, then $[B : A] = [\overline{B} : \overline{A}]$,
3. $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B} \rangle$,
4. $\overline{A \cap B} = \overline{A} \cap \overline{B}$,
5. $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

Example



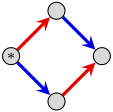
Application: commutator subgroups and abelianizations

We've seen how to divide $\mathbb{Z}$ by $\langle 12 \rangle$, thereby "forcing" all multiples of 12 to be zero. This is one way to construct the integers modulo 12: $\mathbb{Z}_{12} \cong \mathbb{Z}/\langle 12 \rangle$.

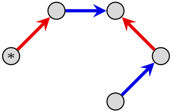
Now, suppose G is nonabelian. We would like to divide G by its "non-abelian parts," making them zero and leaving only "abelian parts" in the resulting quotient.

A commutator is an element of the form $aba^{-1}b^{-1}$. Since G is nonabelian, *there are non-identity commutators: $aba^{-1}b^{-1} \neq e$ in G.*

$ab = ba$



$ab \neq ba$



In this case, the set $C := \{aba^{-1}b^{-1} \mid a, b \in G\}$ contains *more* than the identity.

Define the commutator subgroup G' of G to be

$$G' := \langle aba^{-1}b^{-1} \mid a, b \in G \rangle .$$

This is a normal subgroup of G (homework exercise). If we quotient out by it, we get an abelian group! (Because we have killed every instance of the "$ab \neq ba$ pattern" shown above.)

Commutator subgroups and abelianizations

Definition

The abelianization of G is the quotient group G/G'. This is the group that one gets by "killing off" all nonabelian parts of G.

In some sense, the commutator subgroup G' is the smallest normal subgroup N of G such that G/N is abelian. [Note that G would be the "largest" such subgroup.]

Equivalently, the quotient G/G' is the largest abelian quotient of G. [Note that $G/G \cong \langle e \rangle$ would be the "smallest" such quotient.]

Universal property of commutator subgroups

Suppose $f \colon G \to A$ is a homomorphism to an abelian group A. Then there is a unique homomorphism $h \colon G/G' \to A$ such that $f = hq$:

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "q"'] & & A \\ & G/G' \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

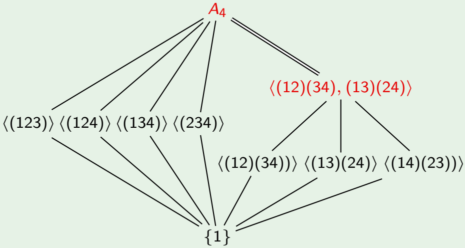
We say that f "factors through" the abelianization, G/G'.

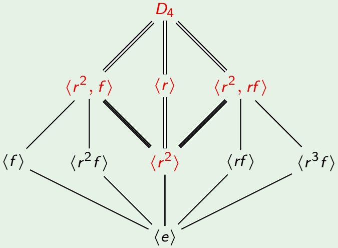
Commutator subgroups and abelianizations

Examples

Consider the groups A_4 and D_4. It is easy to check that

$$G'_{A_4} = \langle xyx^{-1}y^{-1} \mid x, y \in A_4 \rangle \cong V_4 \,, \qquad G'_{D_4} = \langle xyx^{-1}y^{-1} \mid x, y \in D_4 \rangle = \langle r^2 \rangle \,.$$





By the *Correspondence Theorem*, the abelianization of A_4 is $A_4/V_4 \cong C_3$, and the abelianization of D_4 is $D_4/\langle r^2 \rangle \cong V_4$.

Notice that G/G' is abelian, and moreover, taking the quotient of G by *anything above* G' will yield an abelian group.

Automorphisms

Definition

An automorphism is an isomorphism from a group to itself.

The set of all automorphisms of G forms a group, called the automorphism group of G, and denoted $\text{Aut}(G)$.

Remarks.

- An automorphism is determined by where it sends the generators.
- An automorphism ϕ must send generators to generators. In particular, if G is cyclic, then it determines a permutation of the set of (all possible) generators.

Examples

1. There are two automorphisms of $\mathbb{Z}$: the identity, and the mapping $n \mapsto -n$. Thus, $\text{Aut}(\mathbb{Z}) \cong C_2$.
2. There is an automorphism $\phi\colon \mathbb{Z}_5 \to \mathbb{Z}_5$ for each choice of $\phi(1) \in \{1, 2, 3, 4\}$. Thus, $\text{Aut}(\mathbb{Z}_5) \cong C_4$ or V_4. (Which one?)
3. An automorphism ϕ of $V_4 = \langle h, v\rangle$ is determined by the image of h and v. There are 3 choices for $\phi(h)$, and then 2 choices for $\phi(v)$. Thus, $|\text{Aut}(V_4)| = 6$, so it is either $C_6 \cong C_2 \times C_3$, or S_3. (Which one?)

Automorphism groups of $\mathbb{Z}_n$

Definition

The multiplicative group of integers modulo n, denoted $\mathbb{Z}_n^*$ or $U(n)$, is the group

$$U(n) := \{k \in \mathbb{Z}_n \mid \gcd(n,k) = 1\}$$

where the binary operation is multiplication, modulo n.

$U(5) = \{1,2,3,4\} \cong C_4$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$U(6) = \{1,5\} \cong C_2$

	1	5
1	1	5
5	5	1

$U(8) = \{1,3,5,7\} \cong C_2 \times C_2$

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Proposition (homework)

The automorphism group of $\mathbb{Z}_n$ is $\mathrm{Aut}(\mathbb{Z}_n) = \{\sigma_a \mid a \in U(n)\} \cong U(n)$, where

$$\sigma_a \colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_n\,, \qquad \sigma_a(1) = a\,.$$

Automorphisms of D_3

Let's find all automorphisms of $D_3 = \langle r, f \rangle$. We'll see a very similar example to this when we study Galois theory.

Clearly, every automorphism ϕ is completely determined by $\phi(r)$ and $\phi(f)$.

Since automorphisms preserve order, if $\phi \in \mathrm{Aut}(D_3)$, then

$$\phi(e) = e\,, \qquad \phi(r) = \underbrace{r \text{ or } r^2}_{\text{2 choices}}, \qquad \phi(f) = \underbrace{f,\ rf, \text{ or } r^2 f}_{\text{3 choices}}\,.$$

Thus, there are *at most* $2 \cdot 3 = 6$ automorphisms of D_3.

Let's try to define two maps, (i) $\alpha \colon D_3 \to D_3$ fixing r, and (ii) $\beta \colon D_3 \to D_3$ fixing f:

$$\begin{cases} \alpha(r) = r \\ \alpha(f) = rf \end{cases} \qquad\qquad \begin{cases} \beta(r) = r^2 \\ \beta(f) = f \end{cases}$$

I claim that:

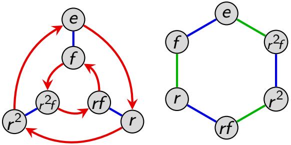
- these both define automorphisms (check this!)
- these generate six *different* automorphisms, and thus $\langle \alpha, \beta \rangle = \mathrm{Aut}(D_3)$.

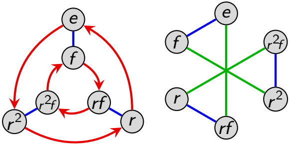
To determine what group this is isomorphic to, find these six automorphisms, and make a group presentation and/or multiplication table. Is it abelian?

Automorphisms of D_3

An automorphism can be thought of as a re-wiring of the Cayley diagram.

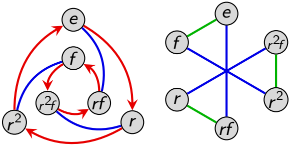
$r \overset{id}{\longmapsto} r$
$f \longmapsto f$

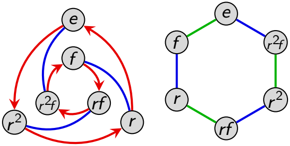




$r \overset{\beta}{\longmapsto} r^2$
$f \longmapsto f$

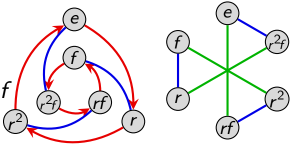
$r \overset{\alpha}{\longmapsto} r$
$f \longmapsto rf$

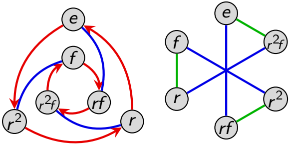




$r \overset{\alpha\beta}{\longmapsto} r^2$
$f \longmapsto r^2 f$

$r \overset{\alpha^2}{\longmapsto} r$
$f \longmapsto r^2 f$



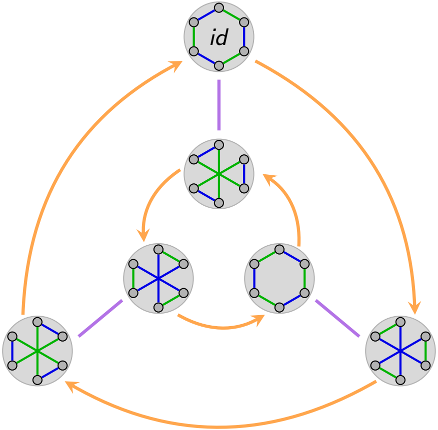


$r \overset{\alpha^2\beta}{\longmapsto} r^2$
$f \longmapsto rf$

Automorphisms of D_3

Here is the multiplication table and Cayley diagram of $\mathrm{Aut}(D_3) = \langle \alpha, \beta \rangle$.

	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
id	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	id	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	id	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	id	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	id	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	id



It is purely coincidence that $\mathrm{Aut}(D_3) \cong D_3$. For example, we've already seen that

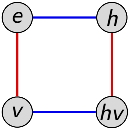
$$\mathrm{Aut}(\mathbb{Z}_5) \cong U(5) \cong C_4\,, \qquad \mathrm{Aut}(\mathbb{Z}_6) \cong U(6) \cong C_2\,, \qquad \mathrm{Aut}(\mathbb{Z}_8) \cong U(8) \cong C_2 \times C_2\,.$$

Automorphisms of $V_4 = \langle h, v \rangle$

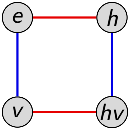
The following permutations are both automorphisms:

α : h v hv and β : h v hv

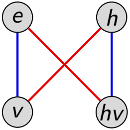
$h \xmapsto{id} h$
$v \longmapsto v$
$hv \longmapsto hv$



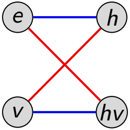
$h \xmapsto{\beta} v$
$v \longmapsto h$
$hv \longmapsto hv$



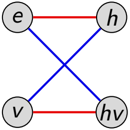
$h \xmapsto{\alpha} v$
$v \longmapsto hv$
$hv \longmapsto h$



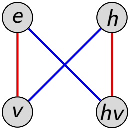
$h \xmapsto{\alpha\beta} h$
$v \longmapsto hv$
$hv \longmapsto v$



$h \xmapsto{\alpha^2} hv$
$v \longmapsto h$
$hv \longmapsto v$



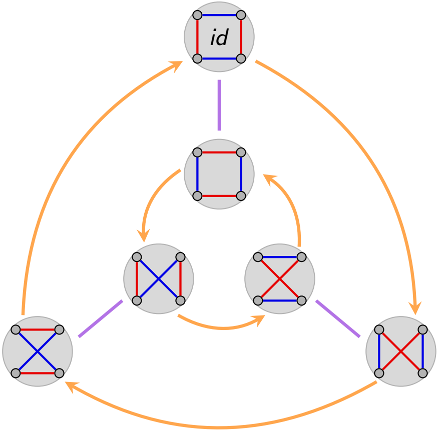
$h \xmapsto{\alpha^2\beta} hv$
$v \longmapsto v$
$hv \longmapsto h$



Automorphisms of $V_4 = \langle h, v \rangle$

Here is the multiplication table and Cayley diagram of $\mathrm{Aut}(V_4) = \langle \alpha, \beta \rangle \cong S_3 \cong D_3$.

	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
id	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	id	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	id	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	id	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	id	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	id



Recall that α and β can be thought of as the permutations 

and 

and so $\mathrm{Aut}(G) \hookrightarrow \mathrm{Perm}(G) \cong S_n$ always holds.