

# Visual Algebra

## Lecture 4.4: Subgroups of quotient groups

**Dr. Matthew Macauley**

School of Mathematical & Statistical Sciences  
Clemson University  
South Carolina, USA  
<http://www.math.clemson.edu/~macaule/>

# The isomorphism theorems

The fundamental homomorphism theorem (FHT) is the first of four basic theorems about homomorphisms and their structure.

These are commonly called “**The isomorphism theorems.**”

- **Fundamental homomorphism theorem:** “*All homomorphic images are quotients*”
- **Correspondence theorem:** Characterizes “*subgroups of quotients*”
- **Fraction theorem:** Characterizes “*quotients of quotients*”
- **Diamond theorem:** “*Duality of subquotients.*”

These all have analogues for other algebraic structures, e.g., rings, vector spaces, modules, Lie algebras.

All of these theorems can look messy and unmotivated algebraically.

However, they all have beautiful visual interpretations, especially involving subgroup lattices.

We just saw the FHT. In this lecture, we'll study the [correspondence theorem](#).

## The correspondence theorem: subgroups of quotients

Given  $N \trianglelefteq G$ , the quotient  $G/N$  has a group structure, via

$$aN \cdot bN = abN.$$

Moreover, by the FHT, every homomorphic image is a quotient.

### Natural question

What are the subgroups of a quotient?

Fortunately, this has a simple answer that is easy to remember.

### Correspondence theorem (informal)

The **subgroups of the quotient**  $G/N$  are **quotients of the subgroups**  $H \leq G$  that contain  $N$ .

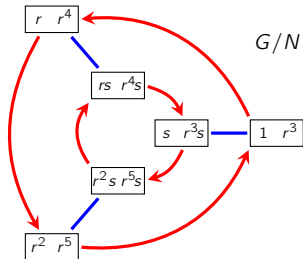
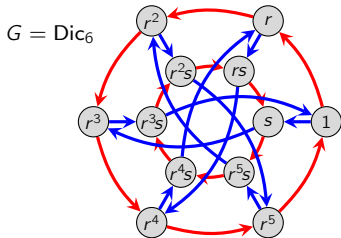
Moreover, “most properties” of  $H/N \leq G/N$  are inherited from  $H \leq G$ .

This is best understood by interpreting the subgroup lattices of  $G$  and  $G/N$ .

Let's do some examples for intuition, and then state the correspondence theorem formally.

# The correspondence theorem: subgroups of quotients

Compare  $G = \text{Dic}_6$  with the quotient by  $N = \langle r^3 \rangle$ .



We know the subgroup structure of  $G/N = \{N, rN, r^2N, sN, rsN, r^2sN\} \cong D_3$ .

“The subgroups of the quotient  $G/N$  are the quotients of the subgroups that contain  $N$ .”

“shoes out of the box”

$r^2$	$r^5$	$r^2s$	$r^5s$
$r$	$r^4$	$rs$	$r^4s$
$1$	$r^3$	$s$	$r^3s$

$$\langle r \rangle \leq G$$

“shoebboxes; lids off”

$r^2$	$r^5$	$r^2s$	$r^5s$
$r$	$r^4$	$rs$	$r^4s$
$1$	$r^3$	$s$	$r^3s$

$$\langle r \rangle / N \leq G/N$$

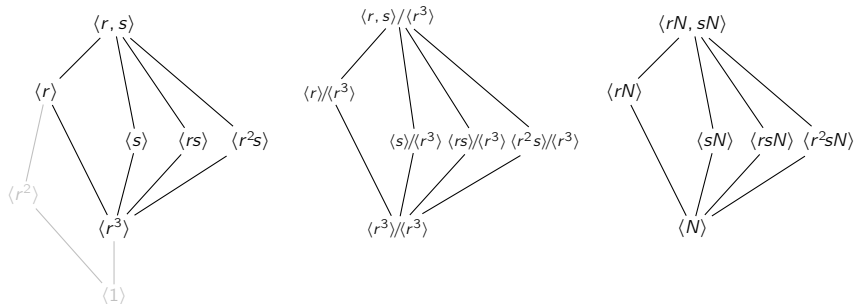
“shoebboxes; lids on”

$r^2N$	$r^2sN$
$rN$	$rsN$
$N$	$sN$

$$\langle rN \rangle \leq G/N$$

## The correspondence theorem: subgroups of quotients

Here is the subgroup lattice of  $G = \text{Dic}_6$ , and of the quotient  $G/N$ , where  $N = \langle r^3 \rangle$ .



*"The subgroups of the quotient  $G/N$  are the quotients of the subgroups that contain  $N$ ."*

*"shoes out of the box"*

$r^2$	$r^5$	$r^2s$	$r^5s$
$r$	$r^4$	$rs$	$r^4s$
1	$r^3$	$s$	$r^3s$

$\langle s \rangle \leq G$

*"shoeboxes; lids off"*

$r^2$	$r^5$	$r^2s$	$r^5s$
$r$	$r^4$	$rs$	$r^4s$
1	$r^3$	$s$	$r^3s$

$\langle s \rangle / N \leq G/N$

*"shoeboxes; lids on"*

$r^2N$	$r^2sN$
$rN$	$rsN$
$N$	$sN$

$\langle sN \rangle \leq G/N$

## The correspondence theorem: subgroups of quotients

### Correspondence theorem (informally)

There is a bijection between subgroups of  $G/N$  and subgroups of  $G$  that contain  $N$ .

“Everything that we want to be true” about the subgroup lattice of  $G/N$  is inherited from the subgroup lattice of  $G$ .

Most of these can be summarized as:

*“The \_\_\_\_\_ of the quotient is just the quotient of the \_\_\_\_\_”*

### Correspondence theorem (formally)

Let  $N \leq H \leq G$  and  $N \leq K \leq G$  be chains of subgroups and  $N \trianglelefteq G$ . Then

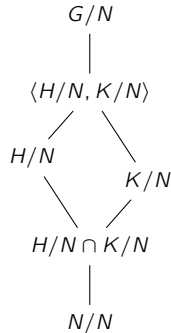
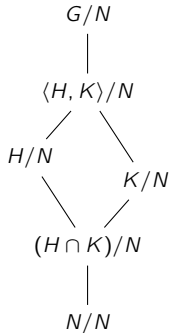
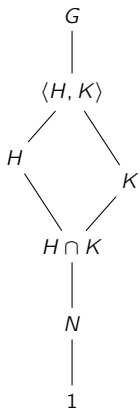
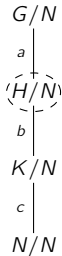
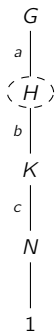
1. Subgroups of the quotient  $G/N$  are quotients of subgroups  $H \leq G$  that contain  $N$ .
2.  $H/N \trianglelefteq G/N$  if and only if  $H \trianglelefteq G$
3.  $[G/N : H/N] = [G : H]$
4.  $H/N \cap K/N = (H \cap K)/N$
5.  $\langle H/N, K/N \rangle = \langle H, K \rangle/N$
6.  $H/N$  is conjugate to  $K/N$  in  $G/N$  iff  $H$  is conjugate to  $K$  in  $G$ .

## The correspondence theorem: subgroups of quotients

All parts of the correspondence theorem have nice subgroup lattice interpretations.

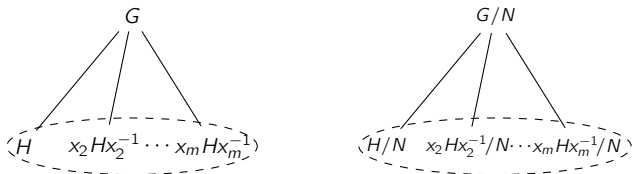
We've already interpreted the first part.

Here's what the next four parts say.

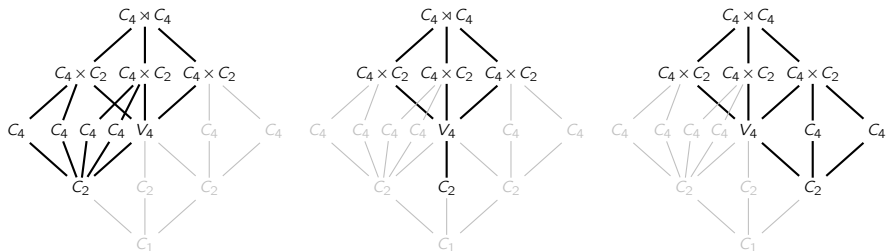


## The correspondence theorem: subgroups of quotients

The last part says that we can characterize the conjugacy classes of  $G/N$  from those of  $G$ .



Let's apply that to find the conjugacy classes of  $C_4 \rtimes C_4$  by inspection alone.





## The correspondence theorem: subgroups of quotients

Let's prove the first (main) part of the correspondence theorem.

### Correspondence theorem (first part)

The subgroups of the quotient  $G/N$  are quotients of subgroups  $H \leq G$  that contain  $N$ .

### Proof

Let  $S$  be a subgroup of  $G/N$ . Then  $S$  is a collection of cosets, i.e.,

$$S = \{hN \mid h \in H\},$$

for some subset  $H \subseteq G$ . We just need to show that  $H$  is a subgroup.

We'll use the **one-step subgroup test**: take  $h_1N, h_2N \in S$ . Then  $S$  must also contain

$$(h_1N)(h_2N)^{-1} = (h_1N)(h_2^{-1}N) = (h_1h_2^{-1})N. \quad (1)$$

That is,  $h_1h_2^{-1} \in H$ , which means that  $H$  is a subgroup. ✓

Conversely, suppose that  $N \leq H \leq G$ . The one-step subgroup test shows that  $H/N \leq G/N$ ; see Eq. (1). □

The other parts are straightforward and will be left as exercises.

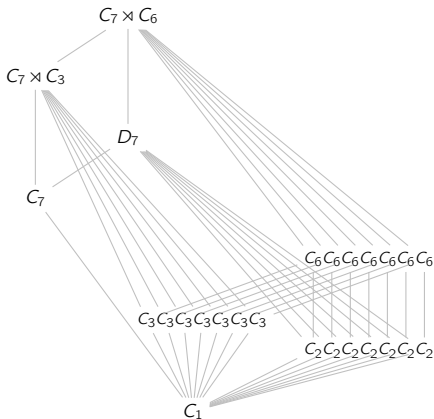
# The quotient $G/Z(G)$ can *never* be a nontrivial cyclic subgroup

Lemma (exercise; see images below)

If  $G/Z(G)$  is cyclic, then  $G$  is abelian.

$$G/Z(G) = \langle \mathbf{gZ} \rangle, \text{ where } Z = Z(G)$$

$\bullet g^{n-1}$	$\bullet g^{n-1}z_1$	$\bullet g^{n-1}z_2$	$\bullet g^{n-1}z_3$	$\dots$	$\mathbf{g^{n-1}Z}$
		$\vdots$			
$\bullet g^2$	$\bullet g^2z_1$	$\bullet g^2z_2$	$\bullet g^2z_3$	$\dots$	$\mathbf{g^2Z}$
$\bullet g$	$\bullet gz_1$	$\bullet gz_2$	$\bullet gz_3$	$\dots$	$\mathbf{gZ}$
$\bullet e$	$\bullet z_1$	$\bullet z_2$	$\bullet z_3$	$\dots$	$\mathbf{Z}$



Note that if  $G$  is abelian, then  $Z(G) = G$ .