

# Subgroups!

Spencer Bagley

With many thanks to Matthew Macauley,  
<http://www.math.clemson.edu/~macaule/>

10 Feb 2025

## Goals for today:

1. Define what subgroups are
2. See some examples
3. Figure out all the subgroups of all the groups of order 4
4. ... of order 6
5. ... of order 8

Definition time!

## Definition time!

Here is the definition of a subgroup.

### Definition

A **subgroup** of  $G$  is a subset  $H \subseteq G$  that is also a group. We denote this by  $H \leq G$ .

Okay, but remind me what's the definition of a group?

### Definition

A **group**  $(G, \star)$  is a set of elements together with a binary operation  $\star$  satisfying the following properties:

1. The operation is associative.
2.  $G$  contains the identity element.
3. Every element in  $G$  has an inverse element.
4.  $G$  is closed under the binary operation.

### Trivial subgroups

Every group  $G$  has the following two boring subgroups:  $G \leq G$ , and  $\{e\} \leq G$ .

### Definition

A **proper subgroup**  $H < G$  is a subgroup that's not equal to the whole group.

# Generating sets

We've previously looked at the **orbit** of an element:

## Definition

The **orbit** of an element  $g \in G$  is the **cyclic subgroup** that it generates,

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\},$$

and its **order** is  $|g| := |\langle g \rangle|$ .

In particular, if  $|g| = n$  is finite, this is the set  $\{g^0 = 1, g, g^2, \dots, g^{n-1}\}$ .

This is a subgroup:

## Cyclic subgroups are subgroups

For any element  $g \in G$ ,  $\langle g \rangle \leq G$ .

But we need not restrain ourselves to generating by one element:

## Definition

Let  $S$  be a **subset** of  $G$ . A **word** in  $S$  is a finite product of finite powers of elements of  $S$  or their inverses.

$\langle S \rangle = \{\text{words in } S\}$  is a subgroup of  $G$ , and it's called the **subgroup generated by  $S$** .

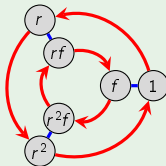
And in fact every subgroup looks like this.

## Example: $C_2 \leq D_3$

Writing  $C_2 \leq D_3$  means *there is a copy of  $C_2$  sitting inside of  $D_3$  as a subgroup.*

### Question

How many ways can you find  $C_2$  sitting inside of  $D_3$ ?



### Remark

It's more precise to express a subgroup by its generator(s).

$$C_2 \cong \langle f \rangle < D_3$$

$$C_2 \cong \langle rf \rangle < D_3$$

$$C_2 \cong \langle r^2f \rangle < D_3$$

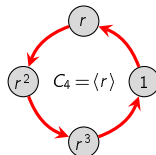
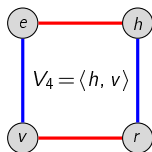
### Question

How about  $C_3 \leq D_3$ ? *There's only one!*

## Groups of order 4

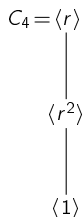
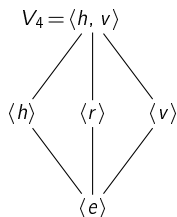
## The two groups of order 4

Let's start by considering the subgroups of the two groups of order 4.



- Proper subgroups of  $V_4$ :  $\langle h \rangle = \{e, h\}$ ,  $\langle v \rangle = \{e, v\}$ ,  $\langle r \rangle = \{e, r\}$ ,  $\langle e \rangle = \{e\}$ .
- Subgroups of  $C_4$ :  $\langle r \rangle = \{1, r, r^2, r^3\} = \langle r^3 \rangle$ ,  $\langle r^2 \rangle = \{1, r^2\}$ ,  $\langle 1 \rangle = \{1\}$ .

It is illustrative to arrange these in a [subgroup lattice](#):



Order: 4

2

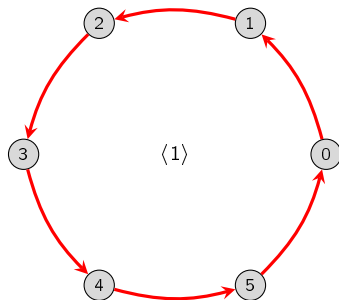
1



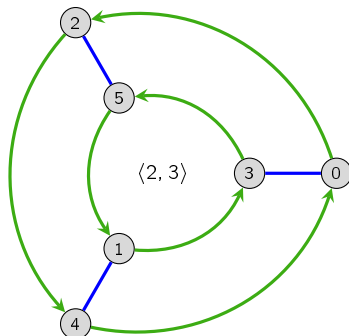
## Groups of order 6

# Subgroups of $\mathbb{Z}_6$

What subgroups can you find in  $\mathbb{Z}_6$ ? I've drawn the Cayley diagram two different ways.

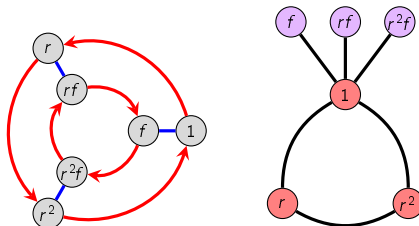


Hello I am secretly also the cycle graph



# Subgroups of $D_3$

Let's figure out all the subgroups of  $D_3$ .



Here are the **non-trivial proper subgroups** of  $D_3$ :

$$\langle r \rangle = \{1, r, r^2\} = \langle r^2 \rangle, \quad \langle f \rangle = \{1, f\}, \quad \langle rf \rangle = \{1, rf\}, \quad \langle r^2f \rangle = \{1, r^2f\}, \quad \langle 1 \rangle = \{1\}.$$

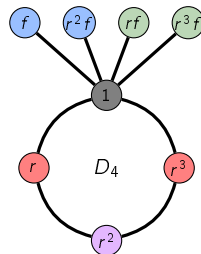
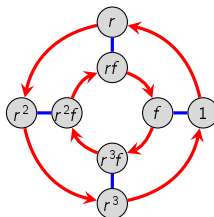
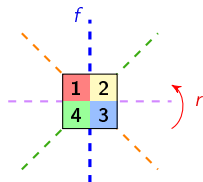
Observations:

- The cycle graph helps us spot cyclic subgroups.
- For small groups like  $D_3$ , the cyclic subgroups may be the **only** proper subgroups.
- There might, however, be more complicated things that are harder to clock.

## Groups of order 8

# Subgroups of $D_4$

See if you can figure out all the subgroups of  $D_4$ .



What do you think is a reasonable way to, like, arrange them?

# Lattices

A **lattice** is a **partially ordered set** such that every pair of elements  $x, y$  has a **unique**:

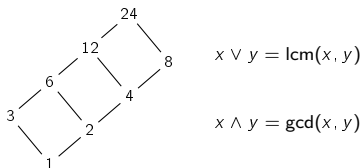
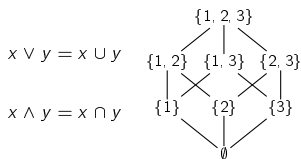
■ **join**, or **sup**, or **least upper bound**

$$x \vee y$$

■ **meet**, or **inf**, or **greatest lower bound**

$$x \wedge y.$$

Examples you may have seen previously are **subset lattices** and **divisor lattices**.



This seems like a good way to organize subgroups, because:

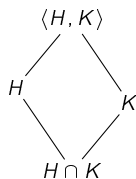
## Theorem

If  $H \leq G$  and  $K \leq G$  are two subgroups, then  $H \cap K$  is a subgroup.  
(Indeed, it's the largest subgroup that's contained in both  $H$  and  $K$ .)

## Theorem

$\langle H, K \rangle$  is the smallest subgroup containing both  $H$  and  $K$ .  
(Note that  $H \cup K$  is not in general a subgroup. Why not?)

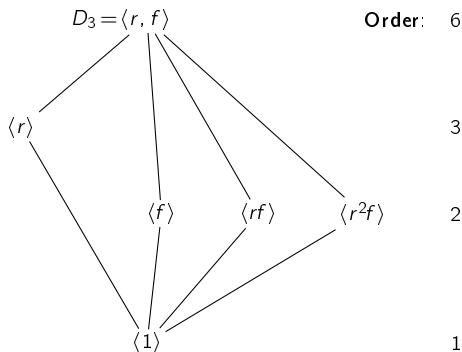
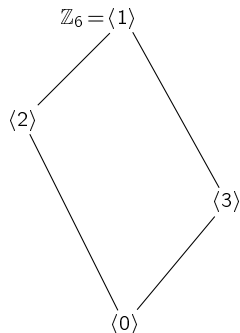
# Subgroup lattices



$H \vee K$ : “smallest subgroup above both  $H$  and  $K$ ”

$H \wedge K$ : “largest subgroup below both  $H$  and  $K$ ”

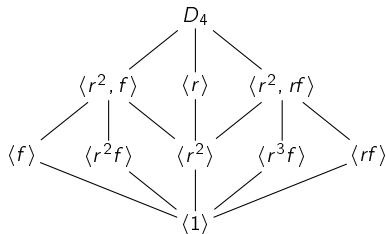
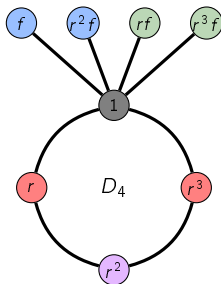
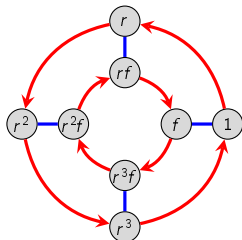
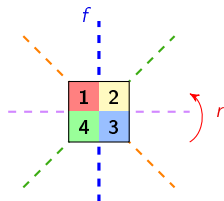
Examples:



# The subgroup lattice of $D_4$

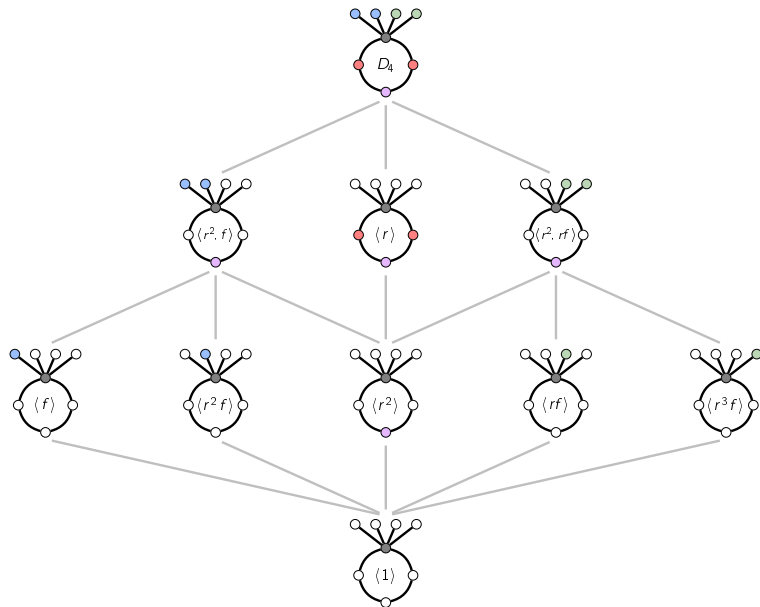
The subgroups of  $D_4$  are:

- The entire group  $D_4$ , and the trivial group  $\langle 1 \rangle$
- 4 subgroups generated by reflections:  $\langle f \rangle$ ,  $\langle rf \rangle$ ,  $\langle r^2 f \rangle$ ,  $\langle r^3 f \rangle$ .
- 1 subgroup generated by a 180° rotation,  $\langle r^2 \rangle \cong C_2$
- 1 subgroup generated by a 90° rotation,  $\langle r \rangle \cong C_4$
- 2 subgroups isomorphic to  $V_4$ :  $\langle r^2, f \rangle$ ,  $\langle r^2, rf \rangle$ .

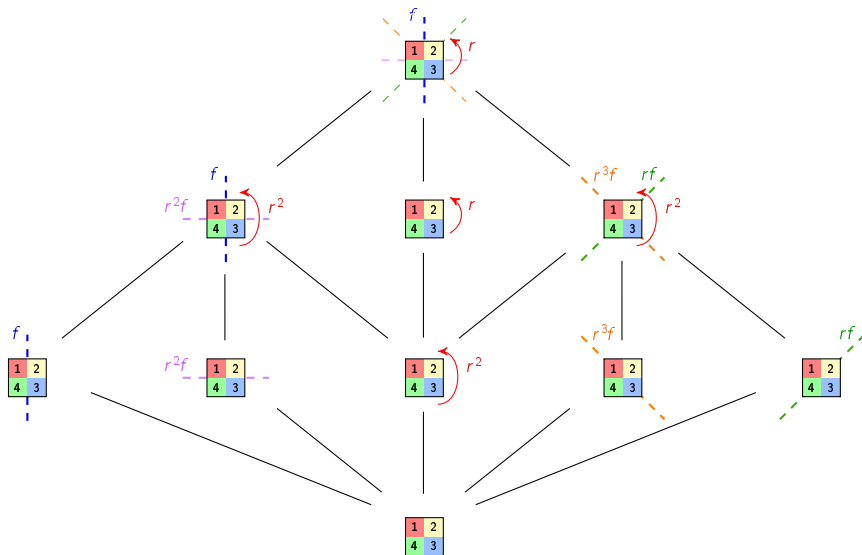




# The subgroup lattice of $D_4$



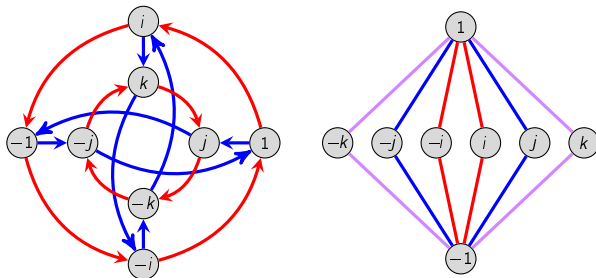
# The subgroup lattice of $D_4$



# The subgroup lattice of $Q_8$

Let's determine all subgroups of the quaternion group

$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle.$$

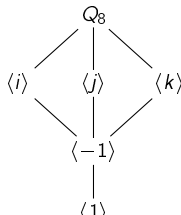


Every element generates a **cyclic subgroup**:

$$\langle 1 \rangle = \{1\}, \quad \langle -1 \rangle = \{\pm 1\}, \quad \langle i \rangle = \langle -i \rangle = \{\pm 1, \pm i\},$$

$$\langle j \rangle = \langle -j \rangle = \{\pm 1, \pm j\}, \quad \langle k \rangle = \langle -k \rangle = \{\pm 1, \pm k\}.$$

Are there any other proper subgroups?



## Subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

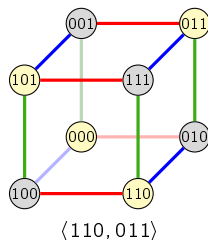
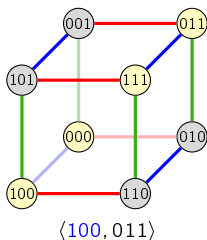
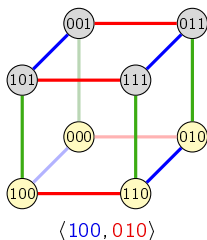
We've seen the subgroup lattices of two groups of order 8:

- $D_4$  has five elements of order 2, and 10 subgroups.
- $Q_8$  has one element of order 2, and 6 subgroups.
- $\mathbb{Z}_2^3$  has seven *elements* of order 2.

### Rule of thumb

Groups with elements of small order tend to have more subgroups than those with elements of large order.

The following Cayley graphs show three different subgroups of order 4 in  $\mathbb{Z}_2^3$ .



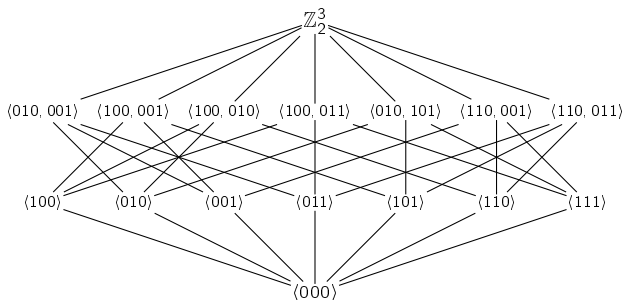
## The subgroup lattice of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

All 7 non-identity elements generate a subgroup isomorphic to  $C_2$ .

All  $\binom{7}{2} = 21$  pairs of non-identity elements generate a subgroup isomorphic to  $V_4$ .

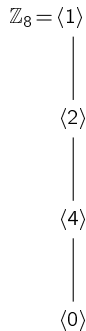
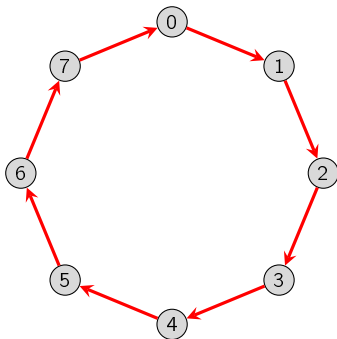
But this triple-counts all such subgroups. In summary, the subgroups of  $\mathbb{Z}_2^3$  are:

- The subgroups  $G$  and  $\{000\}$ ,
- 7 subgroups isomorphic to  $C_2$ ,
- 7 subgroups isomorphic to  $V_4$ .



## The subgroup lattice of $\mathbb{Z}_8$

Draw the Cayley diagram of  $\mathbb{Z}_8$  and find all its subgroups. Arrange them in a lattice.

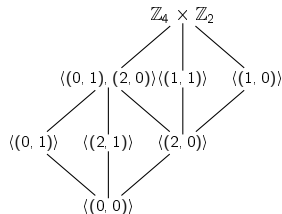
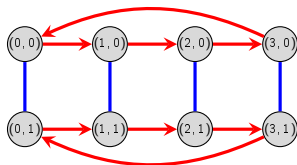


### Theorem

Every subgroup of a cyclic group is cyclic.

## Groups of order 8

There is one more group of order 8, which is  $\mathbb{Z}_4 \times \mathbb{Z}_2$ .



Let's summarize the sizes of the subgroups of the groups of order 8 that we have seen.

	$C_8$	$Q_8$	$C_4 \times C_2$	$D_4$	$C_2^3$
# elts. of order 8	4	0	0	0	0
# elts. of order 4	2	6	4	2	0
# elts. of order 2	1	1	3	5	7
# elts. of order 1	1	1	1	1	1
# subgroups	4	6	8	10	16

### Observations?

- Groups that have more elements of small order tend to have more subgroups.
- In all of these cases, the order of each subgroup divides  $|G|$ .

The end!