Chapter 6: Subgroups

Matthew Macauley

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

Math 4120, Summer I 2014

Overview

In this chapter we will introduce the concept of a subgroup and begin exploring some of the rich mathematical territory that this concept opens up for us.

A subgroup is some smaller group living inside a larger group.

Before we embark on this leg of our journey, we must return to an important property of Cayley diagrams that we've mentioned, but haven't analyzed in depth.

This feature, called *regularity*, will help us visualize the new concepts that we will introduce.

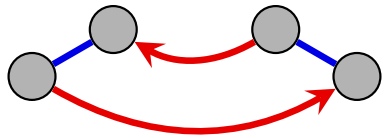
Let's begin with an example.

Regularity

Consider the group D_3. It is easy to verify that $frf = r^{-1}$.

Thus, starting at *any* node in the Cayley diagram, the path frf will *always* lead to the same node as the path r^{-1}.

That is, the following fragment permeates throughout the diagram.



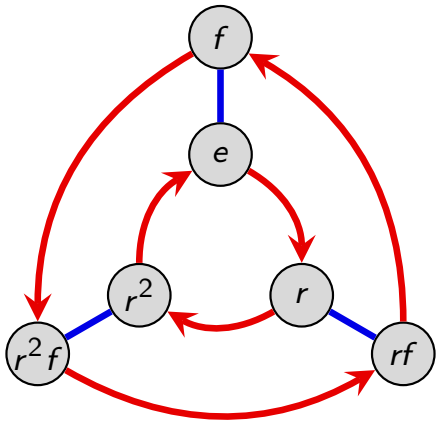
Observe that equivalently, this is the same as saying that the path $frfr$ will always bring you back to where you started. (Because $frfr = e$).

Key observation

The algebraic relations of a group, like $frf = r^{-1}$, give Cayley diagrams a uniform symmetry – every part of the diagram is structured like every other.

Regularity

Let's look at the Cayley diagram for D_3:



Check that indeed, $frf = r^{-1}$ holds by following the corresponding paths starting at any of the six nodes.

There are other patterns that permeate this diagram, as well. Do you see any?

Here are a couple: $f^2 = e$, $r^3 = e$.

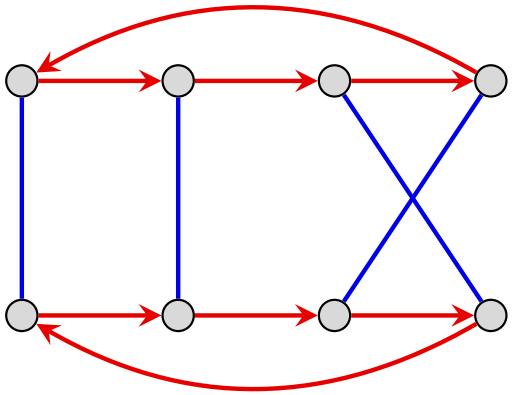
Definition

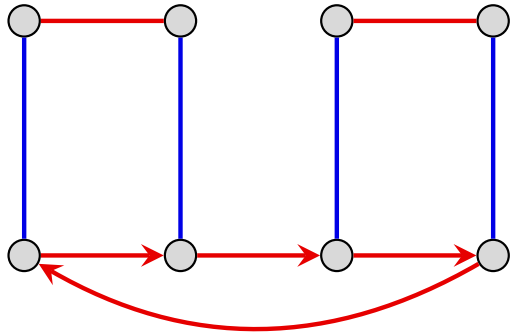
A diagram is called regular if it repeats every one of its interval patterns throughout the whole diagram, in the sense described above.

Regularity

Every Cayley diagram is regular. In particular, diagrams lacking regularity do *not* represent groups (and so they are not called Cayley diagrams).

Here are two diagrams that *cannot* be the Cayley diagram for a group because they are not regular.





Recall that our original definition of a group was informal and "unofficial."

One reason for this is that technically, regularity needs to be incorporated in the rules. Otherwise, the previous diagram would describe a group of actions.

We've indirectly discussed the regularity property of Cayley diagrams, and it was implied, but we haven't spelled out the details until now.

Subgroups

Definition

When one group is contained in another, the smaller group is called a subgroup of the larger group. If H is a subgroup of G, we write $H < G$ or $H \leq G$.

All of the orbits that we saw in Chapter 5 are subgroups. Moreover, they are *cyclic* subgroups. (Why?)

For example, the orbit of r in D_3 is a subgroup of order 3 living inside D_3. We can write

$$\langle r \rangle = \{e, r, r^2\} < D_3.$$

In fact, since $\langle r \rangle$ is really just a copy of C_3, we may be less formal and write

$$C_3 < D_3.$$

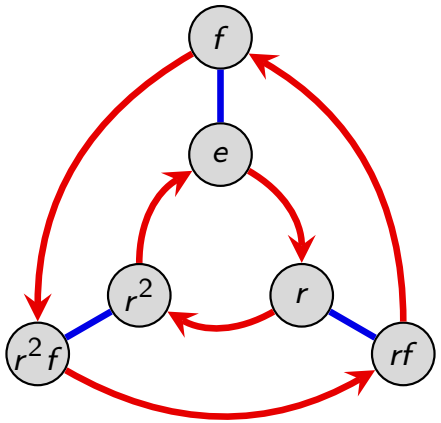
An example: D_3

Recall that the orbits of D_3 are

$$\langle e \rangle = \{e\}, \qquad \langle r \rangle = \langle r^2 \rangle = \{e, r, r^2\}, \qquad \langle f \rangle = \{e, f\}$$

$$\langle rf \rangle = \{e, rf\}, \qquad \langle r^2 f \rangle = \{e, r^2 f\}.$$

The orbits corresponding to the generators are staring at us in the Cayley diagram. The others are more hidden.

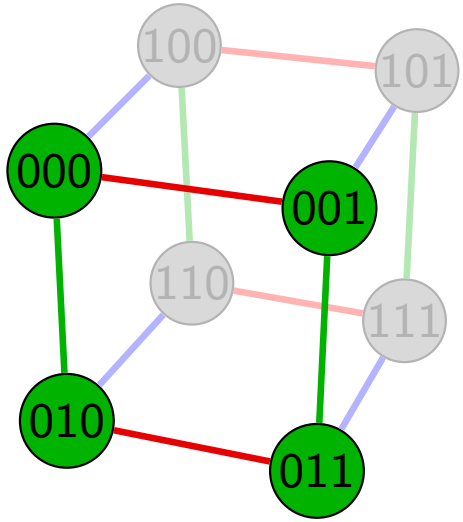


It turns out that all of the subgroups of D_3 are just (cyclic) orbits, but there are many groups that have subgroups that are not cyclic.

Another example: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Here is the Cayley diagram for the group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (the "three-light switch group").

A copy of the subgroup V_4 is highlighted.



The group V_4 requires at least two generators and hence is *not* a cyclic subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. In this case, we can write

$$\langle 001, 010 \rangle = \{000, 001, 010, 011\} < \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Every (nontrivial) group G has *at least* two subgroups:

1. the trivial subgroup: $\{e\}$
2. the non-proper subgroup: G. (Every group is a subgroup of itself.)

Question

Which groups have *only* these two subgroups?

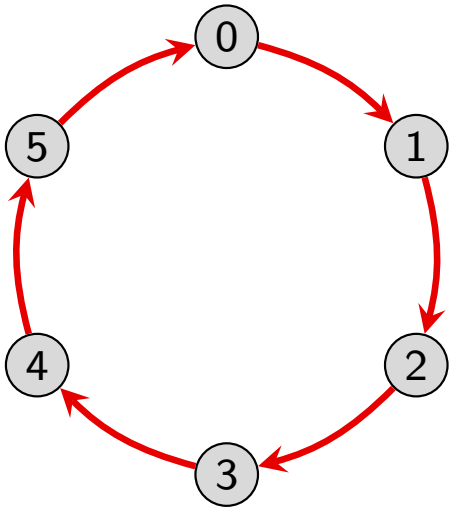
Yet one more example: $\mathbb{Z}_6$

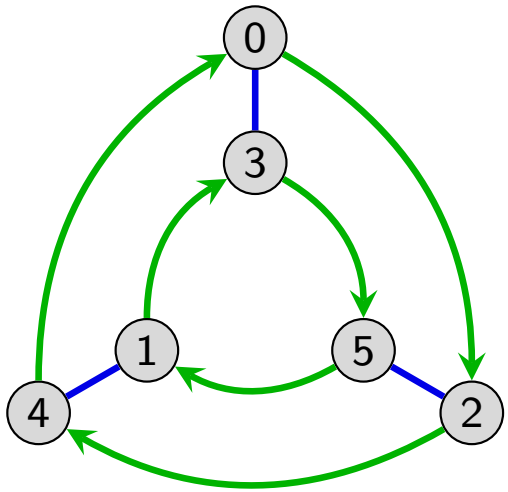
It is not difficult to see that the subgroups of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ are

$$\{0\}, \qquad \langle 2 \rangle = \{0, 2, 4\}, \qquad \langle 3 \rangle = \{0, 3\}, \qquad \langle 1 \rangle = \mathbb{Z}_6.$$

Depending our choice of generators and layout of the Cayley diagram, not all of these subgroups may be "visually obvious."

Here are two Cayley diagrams for $\mathbb{Z}_6$, one generated by $\langle 1 \rangle$ and the other by $\langle 2, 3 \rangle$:





One last example: D_4

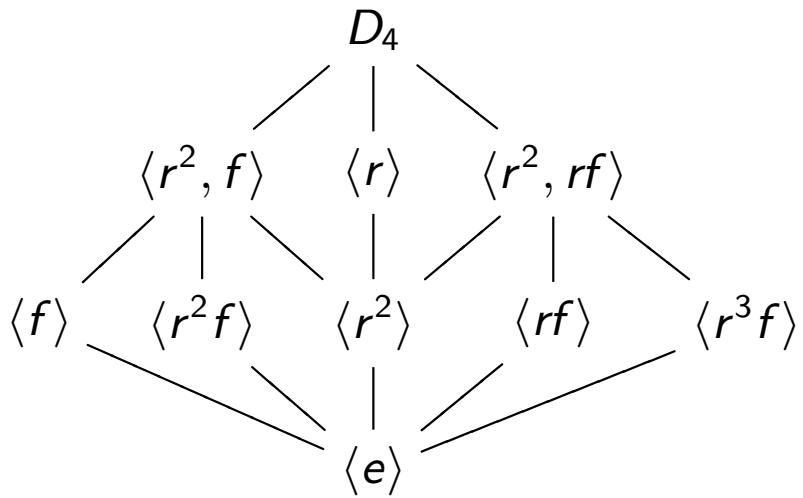
The dihedral group D_4 has 10 subgroups, though some of these are isomorphic to each other:

$$\{e\}, \underbrace{\langle r^2\rangle, \langle f\rangle, \langle rf\rangle, \langle r^2 f\rangle, \langle r^3 f\rangle}_{\text{order 2}}, \underbrace{\langle r\rangle, \langle r^2, f\rangle, \langle r^2, rf\rangle}_{\text{order 4}}, D_4.$$

Remark

We can arrange the subgroups in a diagram called a subgroup lattice that shows which subgroups contain other subgroups. This is best seen by an example.

The subgroup lattice of D_4:



A (terrible) way to find all subgroups

Here is a brute-force method for finding all subgroups of a given group G of order n.

Though this algorithm is horribly inefficient, it makes a good thought exercise.

0. we always have $\{e\}$ and G as subgroups
1. find all subgroups generated by a single element ("cyclic subgroups")
2. find all subgroups generated by 2 elements

$\vdots$

n-1. find all subgroups generated by $n-1$ elements

Along the way, we will certainly duplicate subgroups; one reason why this is so inefficient and impractible.

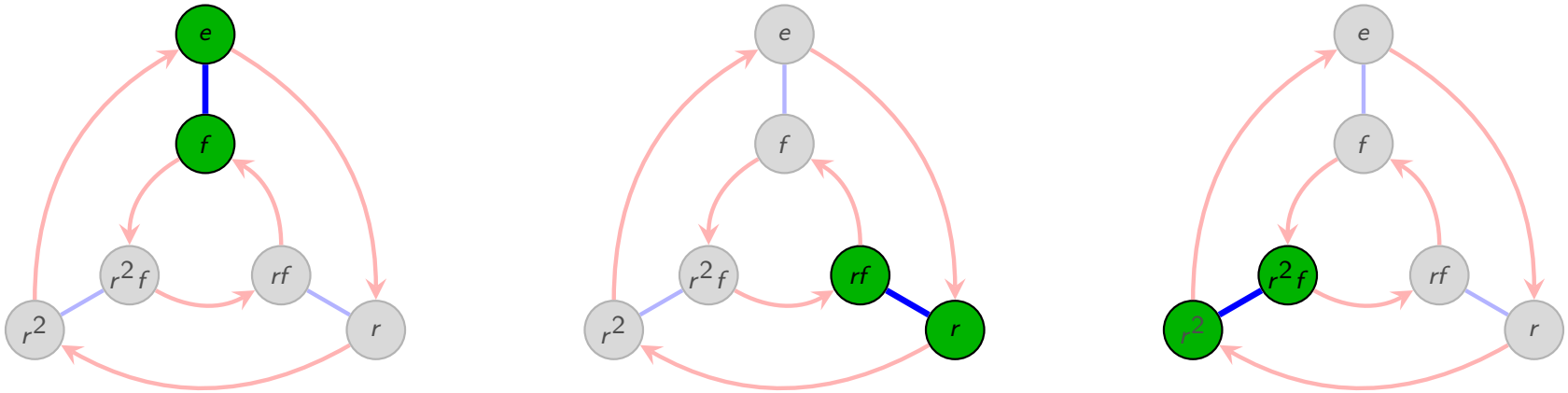
This algorithm works because every group (and subgroup) has a set of generators.

At the end of this chapter, we will see how Lagrange's theorem greatly narrows down the possibilities for subgroups.

Cosets

The regularity property of Cayley diagrams implies that identical copies of the fragment of the diagram that correspond to a subgroup appear throughout the rest of the diagram.

For example, the following figures highlight the repeated copies of $\langle f \rangle = \{e, f\}$ in D_3:



However, only one of these copies is actually a group! Since the other two copies do *not* contain the identity, they cannot be groups.

Key concept

The elements that form these repeated copies of the subgroup fragment in the Cayley diagram are called cosets.

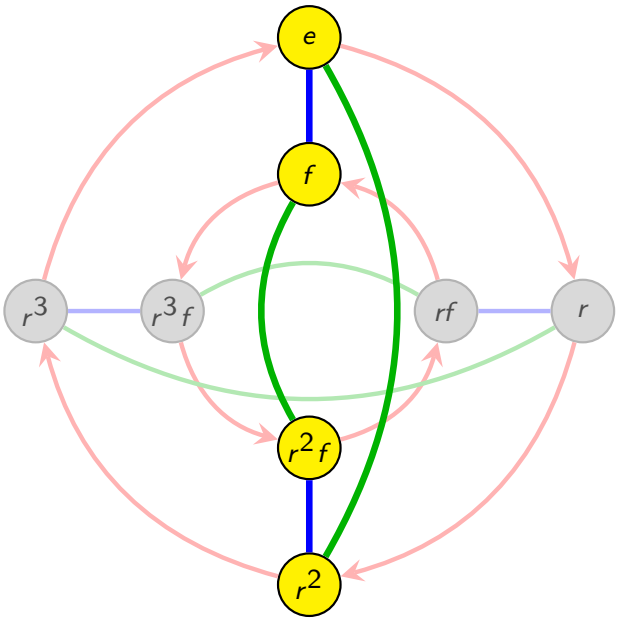
An example: D_4

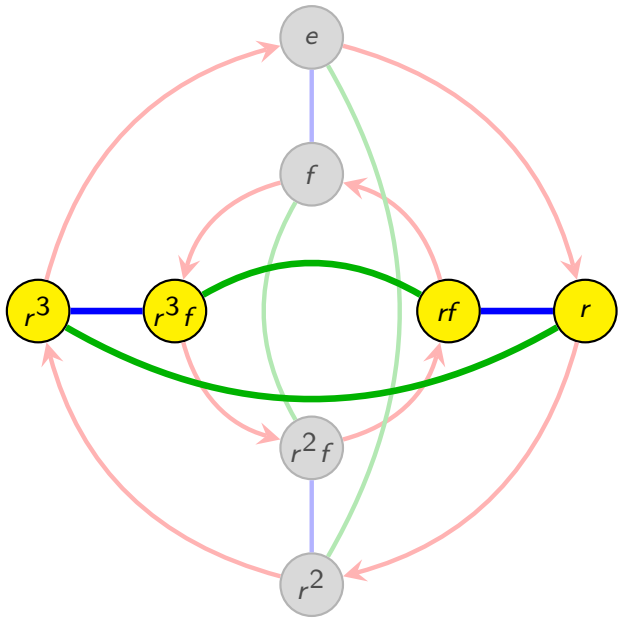
Let's find all of the cosets of the subgroup $H = \langle f, r^2 \rangle = \{e, f, r^2, r^2 f\}$ of D_4.

If we use r^2 as a generator in the Cayley diagram of D_4, then it will be easier to "see" the cosets.

Note that $D_4 = \langle r, f \rangle = \langle r, f, r^2 \rangle$. The cosets of $H = \langle f, r^2 \rangle$ are:

$$H = \langle f, r^2 \rangle = \underbrace{\{e, f, r^2, r^2 f\}}_{\text{original}}, \qquad rH = r\langle f, r^2 \rangle = \underbrace{\{r, r^3, rf, r^3 f\}}_{\text{copy}}.$$





More on cosets

Definition

If H is a subgroup of G, then a (left) coset is a set

$$aH = \{ah : h \in H\},$$

where $a \in G$ is some fixed element. The distingusihed element (in this case, a) that we choose to use to name the coset is called the representative.

Remark

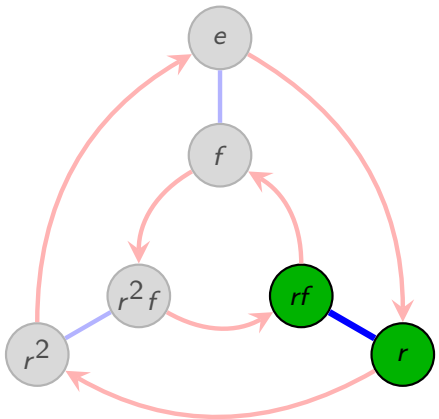
In a Cayley diagram, the (left) coset aH can be found as follows: start from node a and follow *all* paths in H.

For example, let $H = \langle f \rangle$ in D_3. The coset $\{r, rf\}$ of H is the set

$$rH = r\langle f \rangle = r\{e, f\} = \{r, rf\}.$$

Alternatively, we could have written $(rf)H$ to denote the same coset, because

$$rfH = rf\{e, f\} = \{rf, rf^2\} = \{rf, r\}.$$



More on cosets

The following results should be "visually clear" from the Cayley diagrams and the regularity property. Formal algebraic proofs that are not done here will be assigned as homework.

Proposition

For any subgroup $H \leq G$, the union of the (left) cosets of H is the whole group G.

Proof

The element $g \in G$ lies in the coset gH, because $g = ge \in gH = \{gh \mid h \in H\}$. □

Proposition

Each (left) coset can have multiple representatives. Specifically, if $b \in aH$, then $aH = bH$. □

Proposition

All (left) cosets of $H \leq G$ have the same size. □

More on cosets

Proposition

For any subgroup $H \leq G$, the (left) cosets of H partition the group G.

Proof

We know that the element $g \in G$ lies in a (left) coset of H, namely gH. Uniqueness follows because if $g \in kH$, then $gH = kH$. □

Subgroups also have right cosets:

$$Ha = \{ha : h \in H\}.$$

For example, the right cosets of $H = \langle f \rangle$ in D_3 are

$$Hr = \langle f \rangle r = \{e, f\}r = \{r, fr\} = \{r, r^2 f\}$$

(recall that $fr = r^2 f$) and

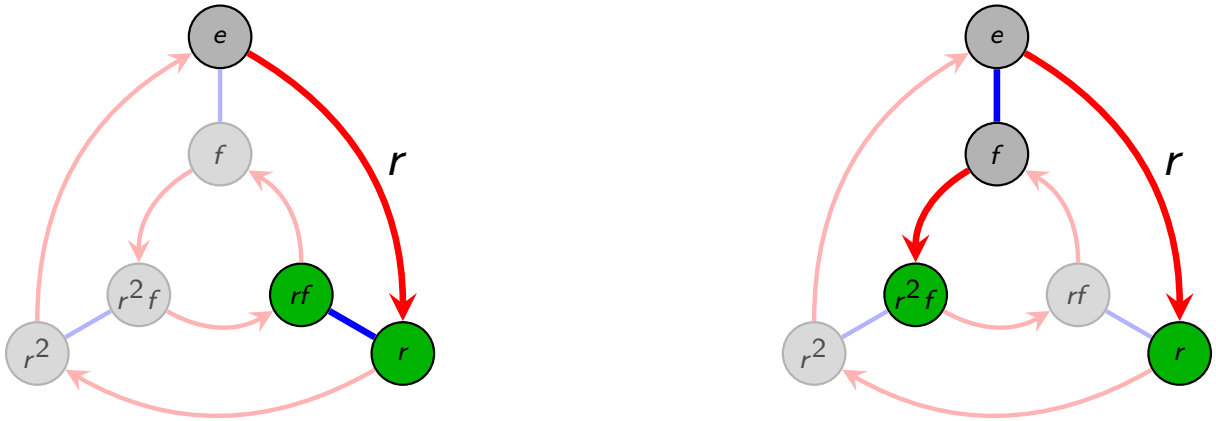
$$\langle f \rangle r^2 = \{e, f\}r^2 = \{r^2, fr^2\} = \{r^2, rf\}.$$

In this example, the left cosets for $\langle f \rangle$ are different than the right cosets. Thus, they must look different in the Cayley diagram.

Left vs. right cosets

The left diagram below shows the left coset $r\langle f \rangle$ in D_3: the nodes that f arrows can reach after the path to r has been followed.

The right diagram shows the right coset $\langle f \rangle r$ in D_3: the nodes that r arrows can reach from the elements in $\langle f \rangle$.



Thus, left cosets look like copies of the subgroup, while the elements of right cosets are usually scattered, because we adopted the convention that arrows in a Cayley diagram represent right multiplication.

Key point

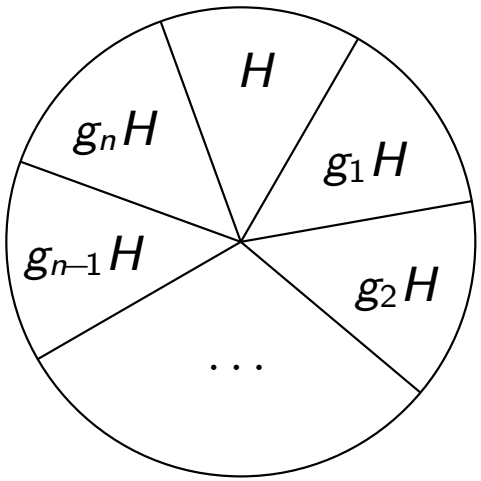
Left and right cosets are generally different.

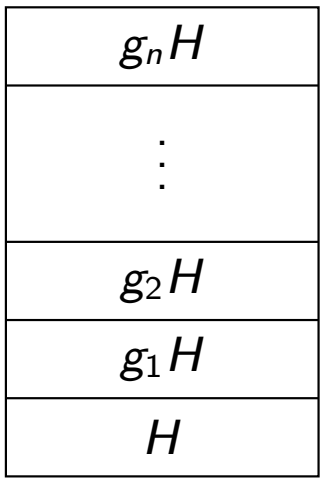
Left vs. right cosets

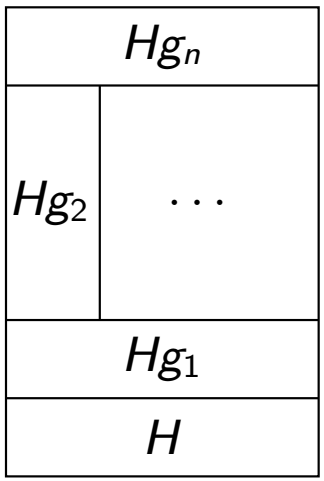
For any subgroup $H \leq G$, we can think of G as the union of non-overlapping and equal size copies of *any* subgroup, namely that subgroup's left cosets.

Though the right cosets also partition G, the corresponding partitions could be different!

Here are a few visualizations of this idea:





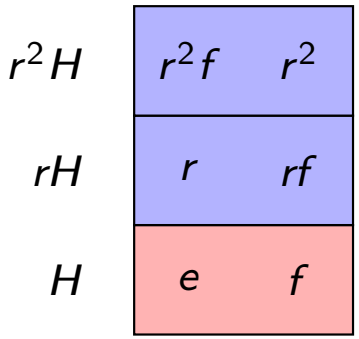


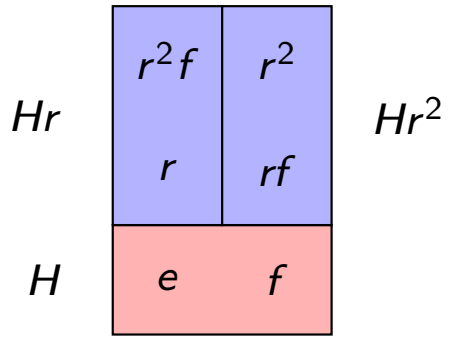
Definition

If $H < G$, then the index of H in G, written $[G : H]$, is the number of distinct left (or equivalently, right) cosets of H in G.

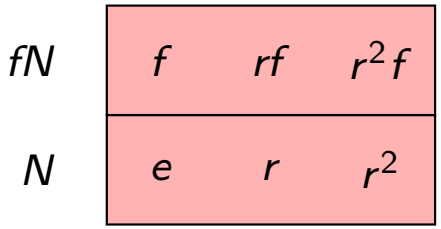
Left vs. right cosets: an example

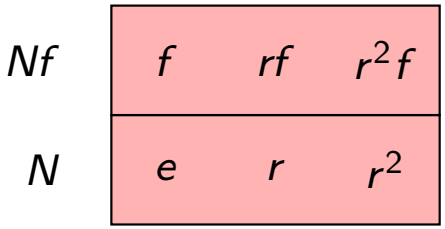
The left and right cosets of the subgroup $H = \langle f \rangle \leq D_3$ are *different*:





The left and right cosets of the subgroup $N = \langle r \rangle \leq D_3$ are *the same*:





Proposition

If $H \leq G$ has index $[G : H] = 2$, then the left and right cosets of H are the same.

Cosets of abelian groups

Recall that in some abelian groups, we use the symbol $+$ for the binary operation.

In this case, left cosets have the form $a + H$ (instead of aH).

For example, let $G = (\mathbb{Z}, +)$, and consider the subgroup $H = 4\mathbb{Z} = \{4k \mid k \in \mathbb{Z}\}$ consisting of multiples of 4.

The left cosets of H are

$$\begin{aligned} H &= \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\} \\ 1 + H &= \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\} \\ 2 + H &= \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\} \\ 3 + H &= \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}. \end{aligned}$$

Notice that these are the same the the right cosets of H:

$$H, \qquad H + 1, \qquad H + 2, \qquad H + 3.$$

Do you see why the left and right cosets of an abelian group will *always* be the same?

Also, note why it would be incorrect to write $3H$ for the coset $3 + H$. In fact, $3H$ would probably be interpreted to be the subgroup $12\mathbb{Z}$.

A theorem of Joseph Lagrange

We are now ready for one of our first major theorems, which is named after the prolific 18th century Italian/French mathematician Joseph Lagrange.

Lagrange's Theorem

Assume G is finite. If $H < G$, then $|H|$ divides $|G|$.

Proof

Suppose there are n left cosets of the subgroup H. Since they are all the same size, and they partition G, we must have

$$|G| = \underbrace{|H| + \cdots + |H|}_{n \text{ copies}} = n|H|.$$

Therefore, $|H|$ divides $|G|$. □

Corollary

If $|G| < \infty$ and $H \leq G$, then

$$[G : H] = \frac{|G|}{|H|}.$$

Normal subgroups

Definition

A subgroup H of G is a normal subgroup of G if $gH = Hg$ for *all* $g \in G$. We denote this as $H \lhd G$, or $H \trianglelefteq G$.

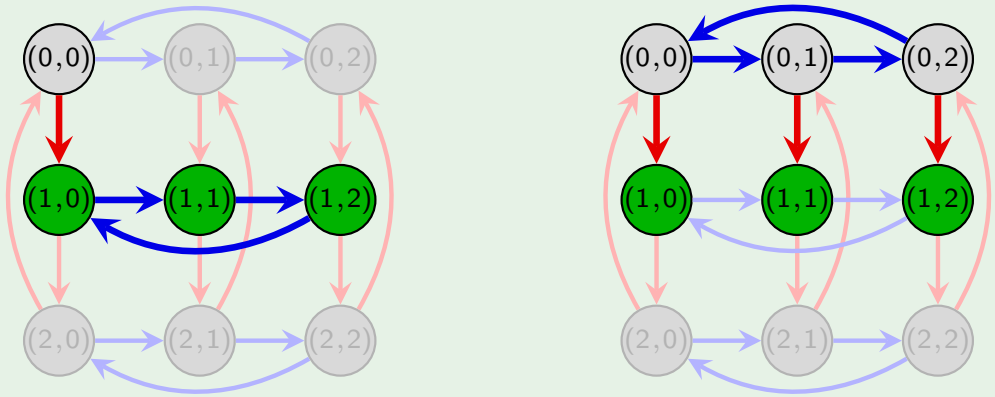
Observation

Subgroups of abelian groups are always normal, because for any $H < G$,

$$aH = \{ah\colon h \in H\} = \{ha\colon h \in H\} = Ha\,.$$

Example

Consider the subgroup $H = \langle(0,1)\rangle = \{(0,0),(0,1),(0,2)\}$ in the group $\mathbb{Z}_3 \times \mathbb{Z}_3$ and take $g = (1,0)$. Addition is done modulo 3, componentwise. The following depicts the equality $g + H = H + g$:



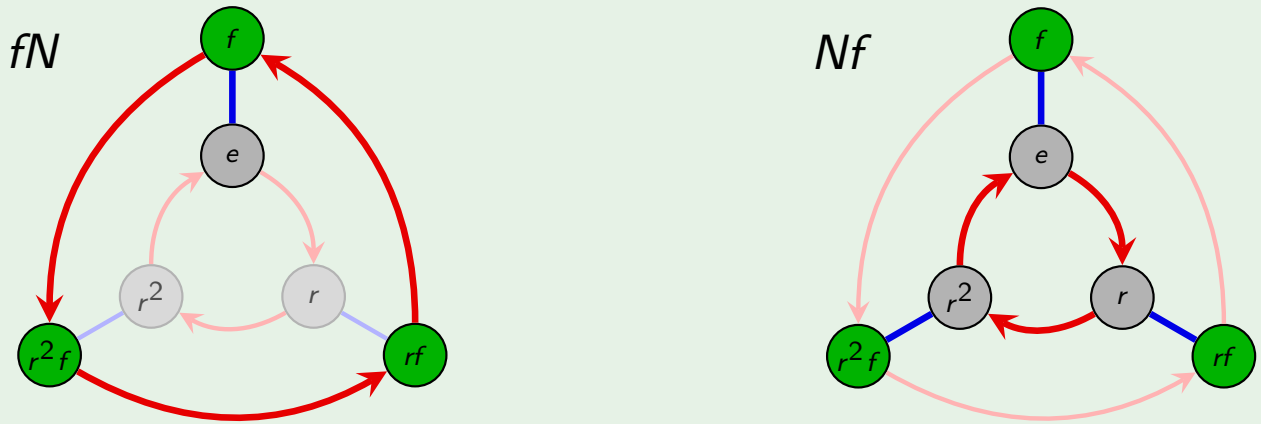
Normal subgroups of nonabelian groups

Since subgroups of abelian groups are always normal, we will be particularly interested in normal subgroups of non-abelian groups.

Example

Consider the subgroup $N = \{e, r, r^2\} \leq D_3$.

The cosets (left or right) of N are $N = \{e, r, r^2\}$ and $Nf = \{f, rf, r^2 f\} = fN$. The following depicts this equality; the coset $fN = Nf$ are the green nodes.



Normal subgroups of nonabelian groups

Here is another way to visualze the normality of the subgroup, $N = \langle r \rangle \leq D_3$:

fN	f	rf	r^2f
N	e	r	r^2

Nf	f	rf	r^2f
N	e	r	r^2

On contrast, the subgroup $H = \langle f \rangle \leq D_3$ is not normal:

r^2H	r^2f	r^2
rH	r	rf
H	e	f

Hr	r^2f	r^2	Hr^2
	r	rf	
H	e	f	

Proposition

If $H \leq G$ has index $[G : H] = 2$, then $H \trianglelefteq G$.

Conjugate subgroups

For a fixed element $g \in G$, the set

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

is called the conjugate of H by g.

Observation 1

For any $g \in G$, the conjugate gHg^{-1} is a subgroup of G.

Proof

1. Identity: $e = geg^{-1}$. ✓
2. Closure: $(gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1}$. ✓
3. Inverses: $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. ✓

□

Observation 2

$gh_1g^{-1} = gh_2g^{-1}$ if and only if $h_1 = h_2$. □

On the homework, you will show that H and gHg^{-1} are isomorphic subgroups. (Though we don't yet know how to do this, or precisely what it means.)

How to check if a subgroup is normal

If $gH = Hg$, then right-multiplying both sides by g^{-1} yields $gHg^{-1} = H$.

This gives us a new way to check whether a subgroup H is normal in G.

Useful remark

The following conditions are all equivalent to a subgroup $H \leq G$ being normal:

(i) $gH = Hg$ for all $g \in G$; ("left cosets are right cosets");

(ii) $gHg^{-1} = H$ for all $g \in G$; ("only one conjugate subgroup")

(iii) $ghg^{-1} \in H$ for all $g \in G$; ("closed under conjugation").

Sometimes, one of these methods is *much* easier than the others!

For example, all it takes to show that H is not normal is finding *one element* $h \in H$ for which $ghg^{-1} \notin H$ for some $g \in G$.

As another example, if we happen to know that G has a unique subgroup of size $|H|$, then H *must* be normal. (Why?)