Lecture 1.1: An introduction to groups

Matthew Macauley

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

Math 8510, Abstract Algebra I

What is a group?

Definition

A nonempty set with an associative binary operation $*$ is a semigroup.

A semigroup S with an identity element 1 such that $1x = x1 = x$ for all $x \in S$ is a monoid.

A group is a monoid G with the property that every $x \in G$ has an inverse $y \in G$ such that $xy = yx = 1$.

Proposition

1. The identity of a monoid is unique.
2. Each element of a group has a unique inverse.
3. If $x, y \in G$, then $(xy)^{-1} = y^{-1}x^{-1}$.

Remarks

- If the binary operation is addition, we write the identity as 0.
- Easy to check that $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{nm}$, $\forall m, n \in \mathbb{Z}$. [Additive analogue?]
- If $xy = yx$ for all $x, y \in G$, then G is said to be abelian.

In this lecture, we'll gain some intuition for groups before we begin a rigorous mathematical treatment of them.

Examples of groups

1. $G = \{1, -1\} \subseteq \mathbb{R}$; multiplication.
2. $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; addition.
3. $G = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$; multiplication. (Also works for $G = \mathbb{R}^*, \mathbb{C}^*$, but *not* $\mathbb{Z}^*$.)
4. $G = \mathrm{Perm}(S)$, the set of *permutations* of S; function composition.

   Special case: $G = S_n$, the set of permutations of $S = \{1, \dots, n\}$.
5. $D_n =$ symmetries of a regular n-gon.
6. $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, where $1 := I_{4\times 4}$ and

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

   Note that $i^2 = j^2 = k^2 = ijk = -1$.
7. Klein 4-group, i.e., the symmetries of a rectangle:

$$V = \{1, v, h, r\} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

8. Symmetries of a frieze diagram, wallpaper, crystal, platonic solid, etc.

Remark. Writing a group G with matrices is called a representation of G. (*What are some advantages of doing this?*)

Cayley diagrams

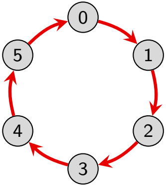
A totally optional, but very useful way to visualize groups, is using a Cayley diagram.

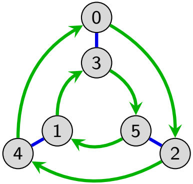
This is a directed graph (G, E), where one *first fixes a generating set* S. We write $G = \langle S \rangle$. Then:

- Vertices: elements of G
- Directed edges: generators.

The vertices can be labeled with elements, with "configurations", or unlabeled.

Example. Two Cayley diagrams for $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} = \langle 1 \rangle = \langle 2, 3 \rangle$:

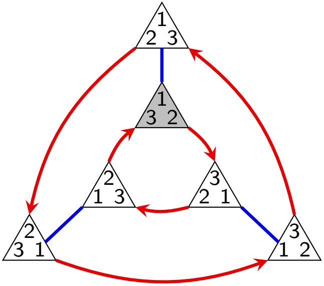




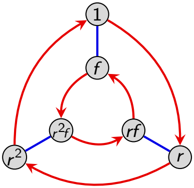
The dihedral group D_3

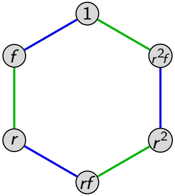
The set $D_3 = \langle r, f \rangle$ of symmetries of an equilateral triangle is a group generated by a clockwise 120° rotation r, and a horizontal flip f.

It can also be generated by f and another reflection g.



Here are two different Cayley diagrams for $D_3 = \langle r, f \rangle = \langle f, g \rangle$, where $g = r^2 f$.



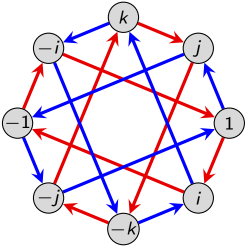


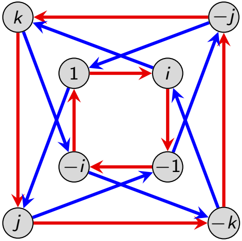
The following are several (of many!) presentations for this group:

$$D_3 = \langle r, f \mid r^3 = f^2 = 1,\ r^2 f = fr \rangle = \langle f, g \mid f^2 = g^2 = (fg)^3 = 1 \rangle.$$

The quaternion group

The following Cayley diagram, laid out two different ways, describes a group of size 8 called the quaternion group, often denoted $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.





The "numbers" j and k individually act like $i = \sqrt{-1}$, because $i^2 = j^2 = k^2 = -1$.

Multiplication of $\{\pm i, \pm j, \pm k\}$ works like the cross product of unit vectors in $\mathbb{R}^3$:

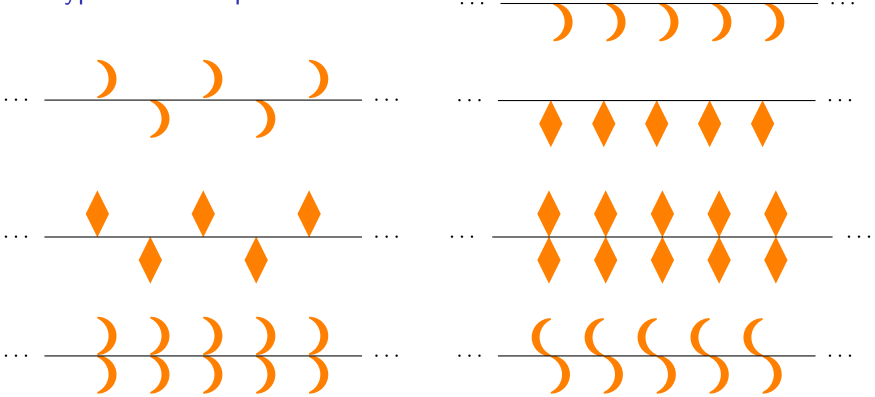
$$ij = k, \quad jk = i, \quad ki = j, \qquad\qquad ji = -k, \quad kj = -i, \quad ik = -j\,.$$

Here are two possible presentations for this group:

$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle = \langle i, j \mid i^4 = j^4 = 1,\ iji = j \rangle\,.$$

Recall that we can alternatvely respresent Q_8 with matrices.

The 7 types of frieze patterns



Remarks

- The symmetry groups of these are generated by some subset of the following symmetries:

$t =$ translation, $g =$ glide reflection, $h =$ horizontal reflection, $v =$ vertical reflection, $r = 180^\circ$ rotation.

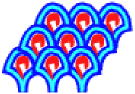
- These 7 symmetric groups fall into 4 classes "up to isomorphism".

The 17 types of wallpaper patterns

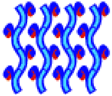
Frieze groups are *one-dimensional symmetry groups*. Two-dimensional symmetry groups are called wallpaper groups.

There are 17 wallpapers groups, shown below, with the official IUC notation, adopted by the International Union of Crystallography in 1952.

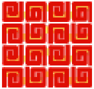
p1



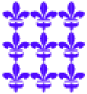
pg



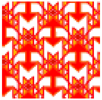
pgg



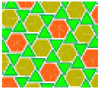
pm



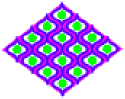
cm



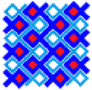
p6



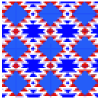
cmm



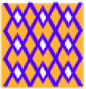
pmg



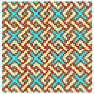
pmm



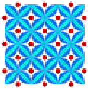
p2



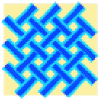
p4



p4m

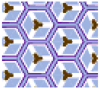


p4g

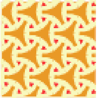


p3

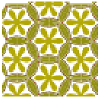
p3m1



p31m

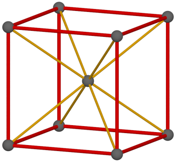


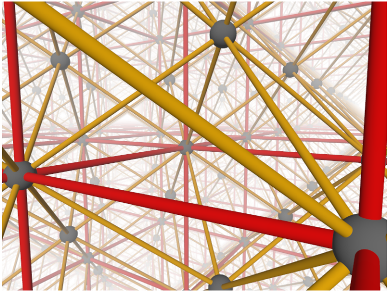
p6m



Crystallography

Three-dimensional symmetry groups are called *crystal groups*. There are 230 crystal groups. One such crystal is shown below.





The study of crystals is called crystallography, and group theory plays a big role is this branch of chemistry.

Subgroups

Definition

A subset $H \subseteq G$ that is a group is called a subgroup of G, and denoted $H \leq G$.

Examples. What are some of the subgroups of the groups we've seen?

1. $G = \{1, -1\} \subseteq \mathbb{R}$; multiplication.
2. $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$; addition.
3. $G = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$; multiplication. (Also works for $G = \mathbb{R}^*, \mathbb{C}^*$, but *not* $\mathbb{Z}^*$.)
4. $G = \mathrm{Perm}(S)$, the set of *permutations* of S; function composition.
   Special case: $G = S_n$, the set of permutations of $S = \{1, \dots, n\}$.
5. $D_n =$ symmetries of a regular n-gon.
6. $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, where $1 := I_{4\times 4}$ and
   $$i = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad j = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad k = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$
   Note that $i^2 = j^2 = k^2 = ijk = -1$.
7. Klein 4-group, i.e., the symmetries of a rectangle:
   $$V = \{1, v, h, r\} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$
8. Symmetries of a frieze diagram, wallpaper, crystal, platonic solid, etc.

Subgroups (proofs done on the board)

Proposition 1.4

A nonempty set $H \subseteq G$ is a subgroup if and only if $xy^{-1} \in H$ for all $x, y \in H$.

Corollary 1.5

If $\{H_\alpha\}$ is any collection of subgroups of G, then $\bigcap_{\alpha} H_\alpha \leq G$.

Every set $S \subseteq G$ generates a subgroup, denoted $\langle S \rangle$. There are two ways to think of this:

- *from the bottom, up*, as "words in $S \cup S^{-1}$", where where $S^{-1} = \{x^{-1} \mid x \in S\}$:

$$\langle S \rangle = \left\{x_1 x_2 \cdots x_k \mid x_i \in S \cup S^{-1}, k \in N\right\}$$

- *from the top, down*: $\langle S \rangle := \bigcap_{S \subseteq H_\alpha \leq G} H_\alpha$.

Think of $\langle S \rangle$ as the "smallest subgroup containing S".

Proposition

$$\left\{x_1, x_2 \cdots x_k \mid x_i \in S \cup S^{-1}, k \in N\right\} = \bigcap_{S \subseteq H_\alpha \leq G} H_\alpha.$$

Cyclic groups (proofs done on the board)

Definition

A group G is cyclic if G is generated by a single element, i.e., if $G = \langle x \rangle$.

Examples

- $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$.
- Rotational symmetries of a regular n-gon, $C_n := \langle r \rangle$. [Or the additive group $(\mathbb{Z}_n, +)$.]

Given $x \in G$, define the order of x to be $|x| := \big|\langle x \rangle\big|$.

Proposition 1.6

Suppose $|x| = n < \infty$ and $x^m = 1$. Then $n \mid m$.

Proposition 1.7

Every subgroup of a cyclic group is cyclic.

Corollary

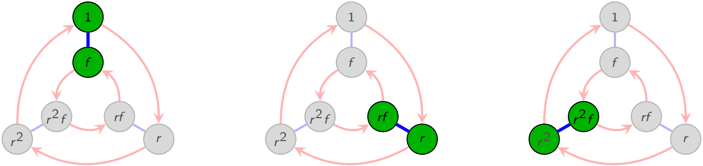
If $G = \langle x \rangle$ of order $n < \infty$, and $k \mid n$, then $\langle x^{n/k} \rangle$ is the *unique* subgroup of order k in G.

Cosets

Definition

If $H \leq G$ and $x, y \in G$, then x and y are congruent mod H, written $x \equiv y \pmod{H}$, if $y^{-1}x \in H$.

Congruent modulo H means "*the difference of x and y lies in H*."



Easy exercise: $\equiv$ is an equivalence relation for any H.

Remark

$x \equiv y \pmod{H}$ means "$x = yh$ *for some* $h \in H$".

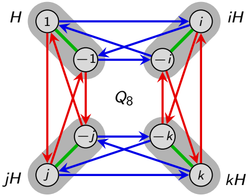
Definition

The equivalence class containing y is $yH := \{yh \mid h \in H\}$, called the left coset of H containing y. Note that $xH = yH$ (as sets) iff $x \equiv y \pmod{H}$.

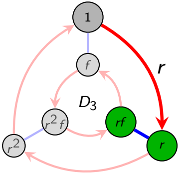
Cosets

Recall that for each $x \in G$, the left coset of H containing x is $xH := \{xh \mid h \in H\}$.

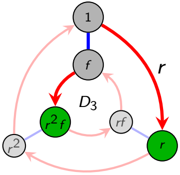
We can similarly define the right coset of H containing x as $Hx := \{hx \mid h \in H\}$.



left cosets of $H = \langle -1 \rangle$
also the rights cosets of H

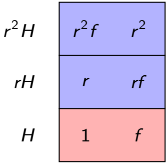


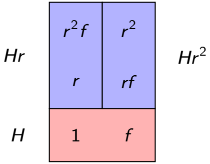
the left coset $r\langle f \rangle$



the right coset $\langle f \rangle r$

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





Cosets

The index of H in G, denoted $[G : H]$ is the number of distinct left cosets of H in G.

Lagrange's theorem

If $H \leq G$, then $|G| = [G : H] \cdot |H|$.

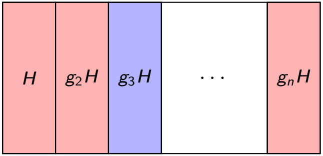
Definition

The normalizer of H in G, denoted $N_G(H)$, is

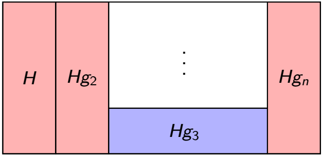
$$N_G(H) = \{g \in G : gH = Hg\} = \{g \in G : gHg^{-1} = H\}.$$

It is easy to check that $H \leq N_G(G) \leq G$.

In the "cartoon" below, the normalizer consists of the elements in the "red cosets".



Partition of G by the left cosets of H



Partition of G by the right cosets of H

Normal subgroups

Definition

A subgroup $H \leq G$ is normal if $gH = Hg$ for all $g \in G$. We write $H \trianglelefteq G$.

Useful remark (exercise)

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").

(iv) $N_G(H) = G$ ("every element normalizes H").

Big idea (exercise)

If $N \triangleleft G$, then there is a well-defined quotient group:

$$G/N := \{xN \mid x \in G\}, \qquad xN \cdot yN := xyN.$$

If G is written additively, then cosets have the form $x + N$, and

$$(x + N) + (y + N) = (x + y) + N.$$

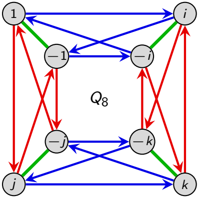
Normal subgroups and quotients

Definition

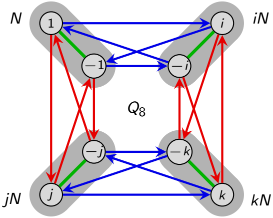
The center of G is the set $Z(G) := \{x \in G \mid xy = yx \text{ for all } y \in G\}$.

It is easy to show that $Z(G) \lhd G$.

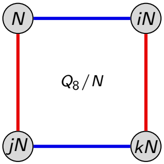
Example. The center of Q_8 is $N = \langle -1 \rangle$. Let's see what the natural quotient $\eta \colon Q_8 \to Q_8/N$ looks like in terms of Cayley diagrams.



Q_8 organized by the subgroup $N = \langle -1 \rangle$



left cosets of N are near each other



collapse cosets into single nodes

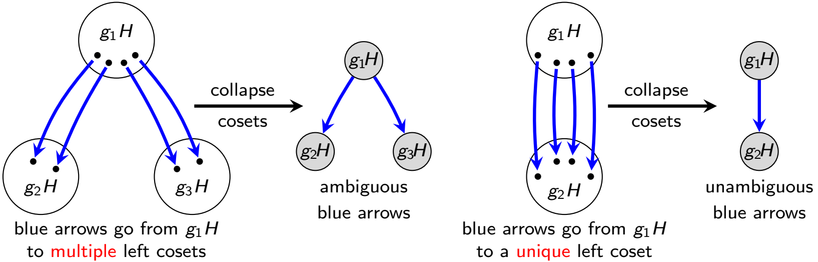
Do you notice any relationship between $Q_8/\operatorname{Ker}(\phi)$ and $\operatorname{Im}(\phi)$?

A visual interpretation of the quotient map being well-defined

Let's try to gain more insight. Consider a group G with subgroup H. Recall that:

- each **left coset** gH is the set of nodes that the H-arrows can reach from g (which looks like a copy of H at g);
- each **right coset** Hg is the set of nodes that the g-arrows can reach from H.

The following figure depicts the potential ambiguity that may arise when cosets are collapsed.



The action of the blue arrows above illustrates multiplication of a left coset on the right by some element. That is, the picture shows how left and right cosets *interact*.

Homomorphisms

Definition

A homomorphism is a function $f \colon G \to H$ such that $f(xy) = f(x)g(y)$ for all $x, y \in G$.

If f is 1–1, it is a monomorphism.

If f is onto, it is an epimormophism.

If f is 1–1 and onto, it is an isomorphism. We say that G and H are isomorphic, and write $G \cong H$.

A homomorphism $f \colon G \to G$ is an endomorphism.

An isomorphism $f \colon G \to G$ is an automorphism.

The kernel of a homomorphism $f \colon G \to H$ is the set $\ker f = \{x \in G \mid f(x) = 1\}$.

Proposition

If $f \colon G \to H$ is a homomorphism, then $\ker f$ is a subgroup of G, and f is 1–1 if and only if $\ker f = \{1\}$.

Homomorphisms

Examples.

1. Let $N \trianglelefteq G$. Then $\eta\colon G \to G/N$, where $\eta\colon g \mapsto gN$ is a homomorphism called the natural quotient.

2. Let $G = (\mathbb{R}, +)$, $H = \{r \in \mathbb{R} \mid r > 0\}$. Then

   $$f\colon G \to H, \qquad f(r) = e^r$$

   is an isomorphism. The inverse map is $f^{-1}\colon H \to G$, $f^{-1}(x) = \ln x$. (Verify this!)

3. Let $G = D_3$, $H = \{-1, 1\}$. Define

   $$f(x) = \begin{cases} 1 & x \text{ is a rotation} \\ -1 & x \text{ is a reflection} \end{cases}$$

   Then f is a homomorphism. (Check!)

4. Let G be abelian and $n \in \mathbb{Z}$. Then

   $$f\colon G \to G, \qquad f(x) = x^n$$

   is an endomorphism, since $(xy)^n = x^n y^n$.

5. Let $G = S_3$, $H = \mathbb{Z}_6$. Then $G \not\cong H$. (Why?)

Automorphisms

Proposition

The set Aut(G) of automorhpisms of G is a group with respect to composition.

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, $\mathrm{Aut}(\mathbb{Z}) \cong C_2$.
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, $\mathrm{Aut}(\mathbb{Z}_5) \cong C_4$ 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, $|\mathrm{Aut}(V_4)| = 6$, 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

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 $\phi \in \text{Aut}(D_3)$, 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:

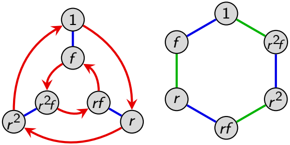
- these both define automorphisms (check this!)
- these generate six *different* automorphisms, and thus $\langle \alpha, \beta \rangle = \text{Aut}(D_3)$.

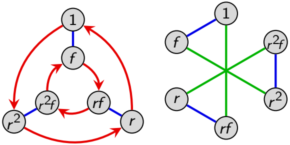
To determine what group this is isomorphic to, find these six automorphisms, and make a group presentation and/or multiplication table. Is it abelian?

Automorphisms of D_3

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

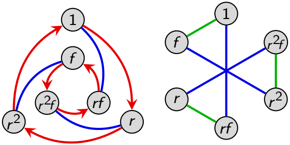
$r \xmapsto{id} r$
$f \longmapsto f$

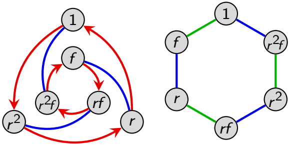




$r \xmapsto{\beta} r^2$
$f \longmapsto f$

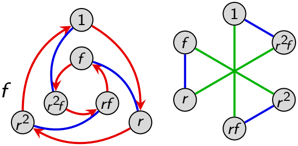
$r \xmapsto{\alpha} r$
$f \longmapsto rf$

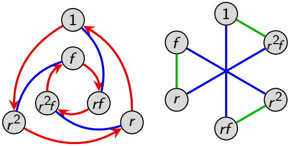




$r \xmapsto{\alpha\beta} r^2$
$f \longmapsto r^2 f$

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



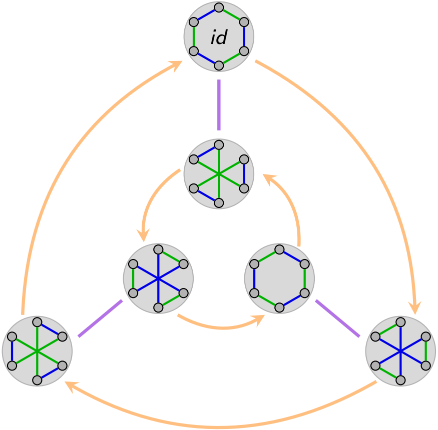


$r \xmapsto{\alpha^2\beta} r^2$
$f \longmapsto rf$

Automorphisms of D_3

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

	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

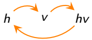


It is purely coincidence that $\text{Aut}(D_3) \cong D_3$. For example, we've already seen that

$$\text{Aut}(\mathbb{Z}_5) \cong U(5) \cong \mathbb{Z}_4\,, \qquad \text{Aut}(\mathbb{Z}_6) \cong U(6) \cong \mathbb{Z}_2\,, \qquad \text{Aut}(\mathbb{Z}_8) \cong U(8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2\,.$$

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

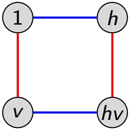
The following permutations are both automorphisms:

α : 

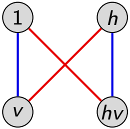
and

β : 

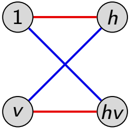
$$h \xrightarrow{id} h$$
$$v \longmapsto v$$
$$hv \longmapsto hv$$



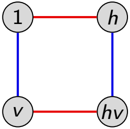
$$h \xrightarrow{\alpha} v$$
$$v \longmapsto hv$$
$$hv \longmapsto h$$



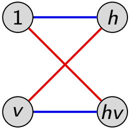
$$h \xrightarrow{\alpha^2} hv$$
$$v \longmapsto h$$
$$hv \longmapsto v$$



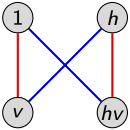
$$h \xrightarrow{\beta} v$$
$$v \longmapsto h$$
$$hv \longmapsto hv$$



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



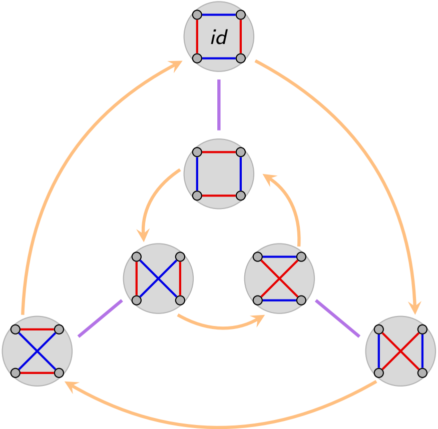
$$h \xrightarrow{\alpha^2\beta} hv$$
$$v \longmapsto v$$
$$hv \longmapsto h$$



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



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

and 

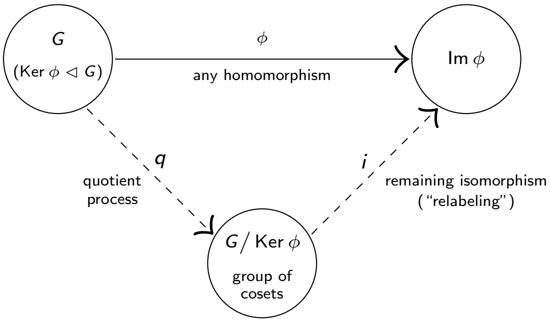
and so $\mathrm{Aut}(G) \hookrightarrow \mathrm{Perm}(G) \cong S_n$ always holds.

The first isomorphism theorem

Fundamental homomorphism theorem (FHT)

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

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

Construct an explicit map $i\colon G/\mathrm{Ker}(\phi) \to \mathrm{Im}(\phi)$ and prove that it is an isomorphism...

The first isomorphism theorem

Fundamental homomorphism theorem (FHT)

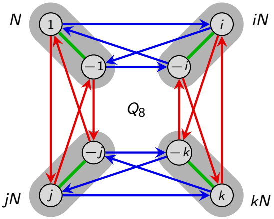
If $\phi\colon G \to H$ is a homomorphism, then $\mathrm{Im}(\phi) \cong G/\operatorname{Ker}(\phi)$.

Let's revist a familiar example to illustrate this. Consider a homomorphism:

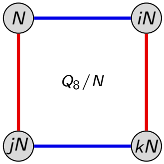
$$\phi\colon Q_8 \longrightarrow V_4, \qquad \phi(i) = h, \quad \phi(j) = v.$$

It is easy to check that $\operatorname{Ker}(\phi) = \langle -1 \rangle \trianglelefteq Q_8$.

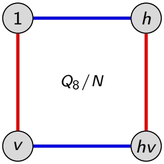
The FHT says that this homomorphism can be done in two steps: (i) quotient by $\langle -1 \rangle$, and then (ii) relabel the nodes accordingly.



left cosets of
$N = \langle -1 \rangle$

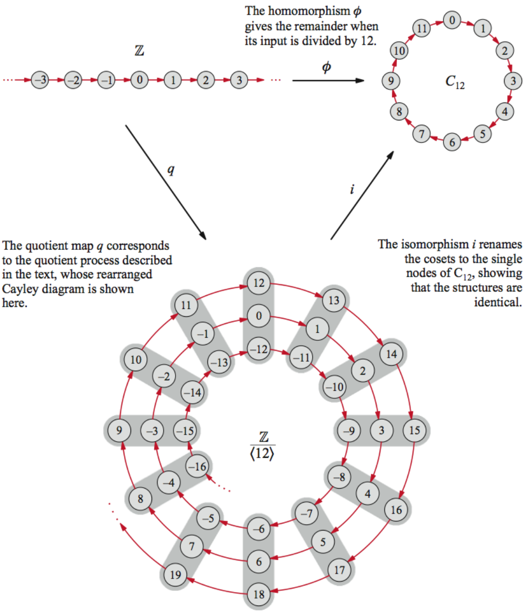


collapse cosets
into single nodes



relabel nodes

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



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 $A, B \lhd G$);
- $G/(A \cap B) \cong (G/A) \times (G/B)$ (assuming $G = AB$).

The Second Isomorphism Theorem

Diamond isomorphism theorem

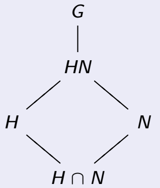
Let $H \leq G$, and $N \lhd N_G(H)$. Then

(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:

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



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.

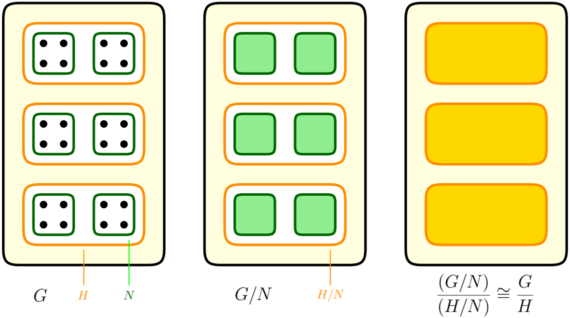
The Third Isomorphism Theorem

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!)

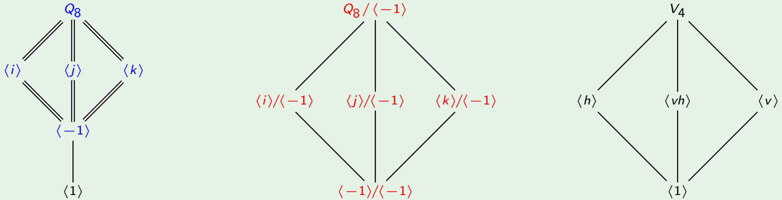
The Fourth Isomorphism Theorem

Correspondence theorem

Let $N \lhd G$. 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 $N \le A \le G$.

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 (full version)

Let $N \lhd G$. 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. $A \lhd G$ if and only if $\overline{A} \lhd \overline{G}$.

Example