Chapter 2: Examples of groups

Matthew Macauley

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

Math 8510, Modern Algebra

Families of groups

In the previous chapter, we encoutered groups meant to appeal to intuition and motivate key concepts. In this chapter, we'll introduce a number of families of groups.

We'll need a diverse collection of go-to examples to keep us grounded. We'll begin with

1. **cyclic groups**: rotational symmetries
2. **abelian groups**: $ab = ba$
3. **dihedral groups**: rotational *and* reflective symmetries
4. **permutation groups**: collections of rearrangements.

Then, by modifying some of our familiar groups, we'll encounter the:

5. **dicyclic** and **generalized quaternion groups**,
6. **diquaternion groups**
7. **semidihedral** and **semiabelian groups**.

Finally, we'll take a tour of:

8. **groups of matrices**
9. **direct products** and **semidirect products** of groups.

We'll see a few other visualization techniques and surprises along the way.

A few basic definitions

Definitions

Let G be a group.

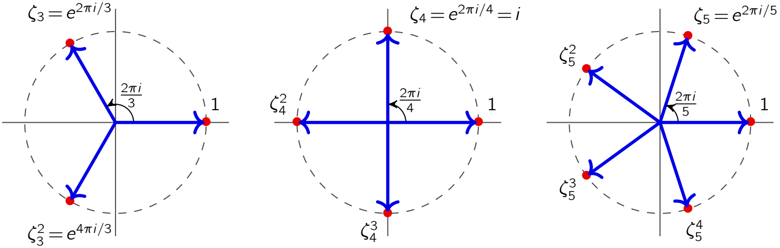
- A subgroup is a subset $H \subseteq G$ that is also a group. We denote this by $H \leq G$.
- The orbit of an element $g \in G$ is the subgroup

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

  and its order is $|g| := \big|\langle g \rangle\big|$. That is, it is either:
  - the minimal $k \geq 1$ such that $g^k = e$, or
  - ∞, if there is no such k.
- the group G is abelian if $ab = ba$ for all $a, b \in G$.

Roots of unity

The polynomial $f(x) = x^n - 1$ has n distinct roots, and they lie on the unit circle.



Definition

For $n \geq 1$, the n^{th} roots of unity are the n roots of $f(x) = x^n - 1$, i.e.,

$$U_n := \left\{\zeta_n^k \mid k = 0, \dots, n-1,\ \zeta_n = e^{2\pi i/n}\right\}.$$

If $\gcd(n, k) = 1$, then ζ_n^k is a primitive n^{th} root of unity.

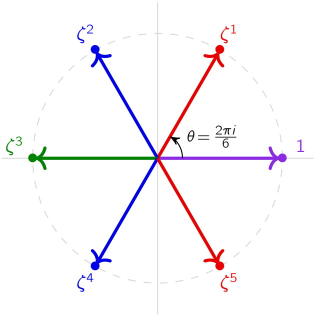
Remark

The n^{th} roots of unity form a group under multiplication.

A motivating example: the 6^{th} roots of unity

The 6^{th} roots of unity are the roots of the polynomial

$$\begin{aligned} x^6-1 &= (x-1)(x^5+x^4+x^3+x^2+x+1) \\ &= (x-1)(x-e^{2\pi i/6})(x-e^{4\pi i/6})(x-e^{6\pi i/6})(x-e^{8\pi i/6})(x-e^{10\pi i/6}) \\ &= (x-1)(x+1)(x^2+x+1)(x^2-x+1) \\ &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) \end{aligned}$$



- $\zeta^0 = e^{0\pi i/6} = 1$: primitive 1^{st} root of unity
- $\zeta^1 = e^{2\pi i/6} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$: primitive 6^{th} root of unity
- $\zeta^2 = e^{4\pi i/6} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$: primitive 3^{rd} root of unity
- $\zeta^3 = e^{6\pi i/6} = -1$: primitive 2^{nd} root of unity
- $\zeta^4 = e^{8\pi i/6} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$: primitive 3^{rd} root of unity
- $\zeta^5 = e^{10\pi i/6} = \frac{1}{2} - \frac{\sqrt{3}}{2}i$: primitive 6^{th} root of unity

Do you see how this generalizes for arbitrary n?

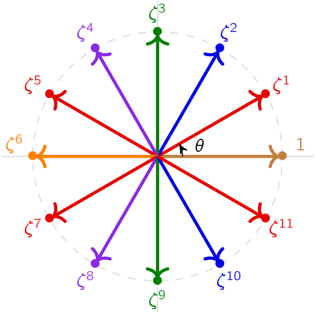
Cyclotomic polynomials

The n^{th} cyclotomic polynomial is $\Phi_n(x) := \prod_{\substack{1 \leq k < n \\ \gcd(n,k)=1}} (x - e^{2\pi i k/n}) = \prod_{\substack{1 \leq k < n \\ \gcd(n,k)=1}} (x - \zeta_n^k)$.

That is, its roots are precisely the primitive n^{th} roots of unity.

An important fact from number theory is that $\Phi_d(x)$ is irreducible and $x^n - 1 = \prod_{0<d|n} \Phi_d(x)$.

$$\begin{aligned} x^{12} - 1 &= \Phi_{12}(x)\,\Phi_6(x)\,\Phi_4(x)\,\Phi_3(x)\,\Phi_2(x)\,\Phi_1(x) \\ &= (x^4 - x^2 + 1)(x^2 - x + 1)(x^2 + 1)(x^2 + x + 1)(x + 1)(x - 1) \end{aligned}$$



- primitive 12^{th} roots of unity: ζ^1, ζ^5, ζ^7, ζ^{11}
- primitive 6^{th} roots of unity: ζ^2, ζ^{10}
- primitive 4^{th} roots of unity: ζ^3, ζ^9
- primitive 3^{rd} roots of unity: ζ^4, ζ^8
- primitive 2^{nd} root of unity: ζ^6
- primitive 1^{st} root of unity: $\zeta^0 = 1$.

Remark

Primitive d^{th} roots of unity: $\{\zeta^k \mid \gcd(n,k) = n/d\}$.

Cyclic groups

Definition

A group is cyclic if it can be generated by a single element.

Here are five ways to represent cyclic groups.

1. As an additive group, modulo n:
$$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}.$$
2. As a multiplicative group:
$$C_n := \{1, r, \ldots, r^{n-1}\} = \langle r \mid r^n = 1 \rangle.$$
3. By roots of unity:
$$C_n \cong \langle \zeta_n \rangle = \langle e^{2\pi i/n} \rangle = \{e^{2\pi ik/n} \mid k = 0, \ldots n-1\} \subseteq \mathbb{C}.$$
4. By real rotation matrices:
$$C_n \cong \langle A_{2\pi/n} \rangle = \left\langle \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix} \right\rangle.$$
5. By complex rotation matrices:
$$C_n \cong \langle R_n \rangle = \left\langle \begin{bmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{bmatrix} \right\rangle = \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix} \right\rangle.$$

Minimal vs. minimum generating sets

Exercise

A number $k \in \{0, 1, \ldots, n-1\}$ generates $\mathbb{Z}_n$ if and only if $\mathbf{gcd}(n, k) = 1$.

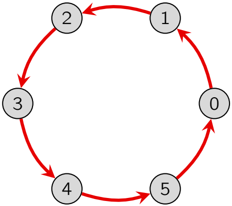
Equivalently, $C_n = \langle \zeta_n^k \rangle$ if and only if $\zeta_n^k = e^{2\pi i k/n}$ is a primitive n^{th} root of unity.

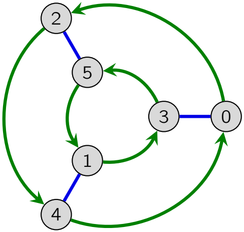
Definition

Given $G = \langle S \rangle$, the set S is a minimal generating set if $T \subsetneq S$ implies $\langle T \rangle \neq G$.

It is minimum if it is minimal, and if for every other generating set T, we have $|S| \leq |T|$.

Here are two minimal generating sets of $\mathbb{Z}_6$:





Infinite cyclic groups

Definition

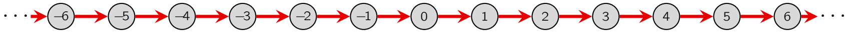
The additive infinite cyclic group is

$$\mathbb{Z} = \langle 1 \mid \quad \rangle,$$

the integers under addition. The multiplicative infinite cyclic group is

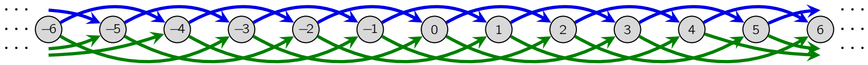
$$C_\infty := \langle r \mid \ \rangle = \{ r^k \mid k \in \mathbb{Z} \}.$$

Several of our frieze groups were cyclic.



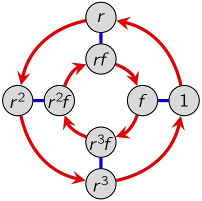
There are only two choices for a minimum generating set: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

There are many choices for larger minimal generating sets. Here is $\mathbb{Z} = \langle 2, 3 \rangle$:

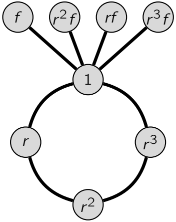


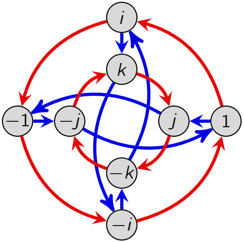
Cycle graphs

We can visualize the orbits in G by the (undirected) cycle graph.

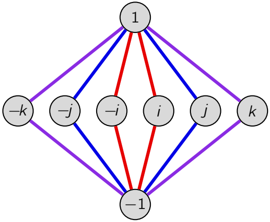


element	orbit
1	$\{1\}$
r^2	$\{1, r^2\}$
r r^3	$\{1, r, r^2, r^3\}$
f	$\{1, f\}$
rf	$\{1, rf\}$
r^2f	$\{1, r^2f\}$
r^3f	$\{1, r^3f\}$





element	orbit
1	$\{1\}$
-1	$\{\pm 1\}$
i $-i$	$\{\pm 1, \pm i\}$
j $-j$	$\{\pm 1, \pm j\}$
k $-k$	$\{\pm 1, \pm k\}$



Unlike Cayley graphs, these do not depend on the generating set!

Dihedral groups

Definition

The dihedral group D_n is the group of symmetries of a regular n-gon. It has order $2n$.

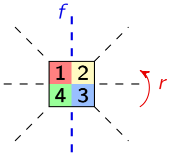
One possible choice of generators is

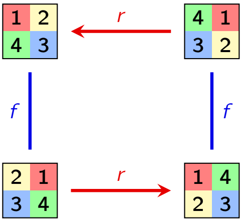
1. $r =$ counterclockwise rotation by $2\pi/n$ radians,
2. $f =$ flip across a fixed axis of symmetry.

We will usually write elements of $D_n = \langle r, f \rangle$ as

$$D_n = \{\underbrace{1, r, r^2, \dots, r^{n-1}}_{n \text{ rotations}}, \underbrace{f, rf, r^2f, \dots, r^{n-1}f}_{n \text{ reflections}}\}.$$

It is easy to check that $rf = fr^{-1}$:

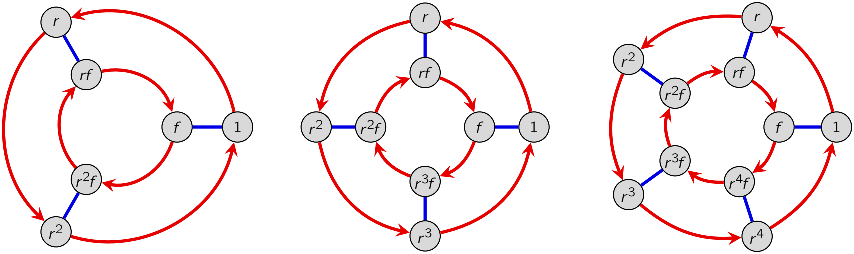




Dihedral groups

Several different presentations for D_n are:

$$D_n = \langle r, f \mid r^n = 1,\ f^2 = 1,\ rfr = f \rangle = \langle r, f \mid r^n = 1,\ f^2 = 1,\ rf = fr^{n-1} \rangle.$$



Warning!

Many books denote the symmetries of the n-gon as D_{2n}.

A strong advantage to our convention is that we can write

$$C_n = \langle r \rangle = \{1, r, r^2, \dots, r^{n-1}\} \leq \langle r, f \rangle = D_n.$$

Dihedral groups

Another way to generate D_n is with adjacent reflections:

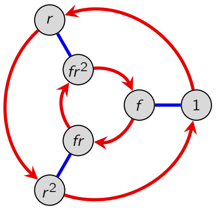
- $s := f$
- $t := fr = r^{n-1}f$

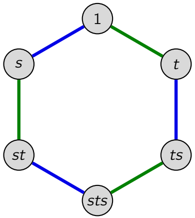
Composing these in either order is a rotation of $2\pi/n$ radians:

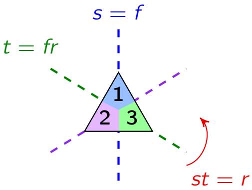
$$st = f(fr) = r, \qquad ts = (fr)f = (r^{n-1}f)f = r^{n-1}.$$

A presentation with these generators is

$$D_n = \langle s, t \mid s^2 = 1,\ t^2 = 1,\ (st)^n = 1 \rangle = \{ \underbrace{1, st, ts, (st)^2, (ts)^2, \dots,}_{\text{rotations}} \underbrace{s, t, sts, tst, \dots}_{\text{reflections}} \}.$$





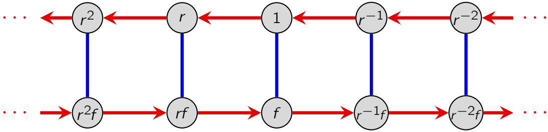


Dihedral groups

Definition

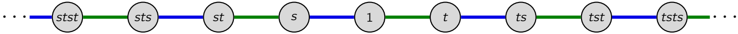
The infinite dihedral group, denoted D_∞, has presentation

$$D_\infty = \langle r, f \mid f^2 = 1,\ rfr = f \rangle.$$



We can also generate D_∞ with two reflections, $s := f$ and $t = fr$.

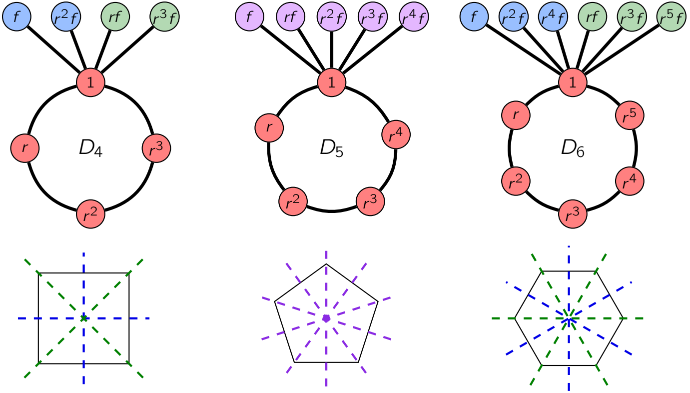
$$D_\infty = \langle s, t \mid s^2 = 1,\ t^2 = 1 \rangle = \{ \underbrace{1, st, ts, (st)^2, (ts)^2, \dots,}_{\text{“rotations”}} \underbrace{s, t, sts, tst, \dots}_{\text{“reflections”}} \}.$$



Cycle graphs of dihedral groups

The maximal orbits of D_n consist of

- 1 orbit of size n containing $\{1, r, \dots, r^{n-1}\}$;
- n orbits of size 2 containing $\{1, r^k f\}$ for $k = 0, 1, \dots, n-1$.



Cayley tables of dihedral groups

The separation of D_n into rotations and reflections is visible in its Cayley tables.

	1	r	r^2	r^3	f	rf	r^2f	r^3f
1	1	r	r^2	r^3	f	rf	r^2f	r^3f
r	r	r^2	r^3	1	rf	r^2f	r^3f	f
r^2	r^2	r^3	1	r	r^2f	r^3f	f	rf
r^3	r^3	1	r	r^2	r^3f	f	rf	r^2f
f	f	r^3f	r^2f	rf	1	r^3	r^2	r
rf	rf	f	r^3f	r^2f	r	1	r^3	r^2
r^2f	r^2f	rf	f	r^3f	r^2	r	1	r^3
r^3f	r^3f	r^2f	rf	f	r^3	r^2	r	1

	1	r	r^2	r^3	f	rf	r^2f	r^3f
1	1	r	r^2	r^3	f	rf	r^2f	r^3f
r	r	r^2	r^3	1	rf	r^2f	r^3f	f
r^2	r^2	r^3	1	r	r^2f	r^3f	f	rf
r^3	r^3	1	r	r^2	r^3f	f	rf	r^2f
f	f	r^3f	r^2f	rf	1	r^3	r^2	r
rf	rf	f	r^3f	r^2f	r	1	r^3	r^2
r^2f	r^2f	rf	f	r^3f	r^2	r	1	r^3
r^3f	r^3f	r^2f	rf	f	r^3	r^2	r	1

rotation	**reflection**
reflection	**rotation**

The partition of D_n as depicted above has the structure of group C_2.

This is another exmaple of a quotient.

We say that $D_4/\langle r\rangle \cong C_2$.

	1	f
1	1	f
f	f	1

Representations of dihedral groups

Recall that the Klein 4-group can be represented by

$$V_4 \cong \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}.$$

Moreover, a rotation of $2\pi/n$ radians can be

$$A_{2\pi/n} = \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix} \qquad \text{or} \qquad R_n := \begin{bmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{bmatrix} = \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix}.$$

The canonical real representation of D_n with 2×2 matrices is

$$D_n \cong \left\langle \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle.$$

The canonical complex representations of D_n with 2×2 matrices is

$$D_n \cong \left\langle \begin{bmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle = \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle.$$

Viewing the groups C_n and D_n as matrices makes our choice of calling the dihedral group D_n (rather than D_{2n}) much more natural!

Direct products

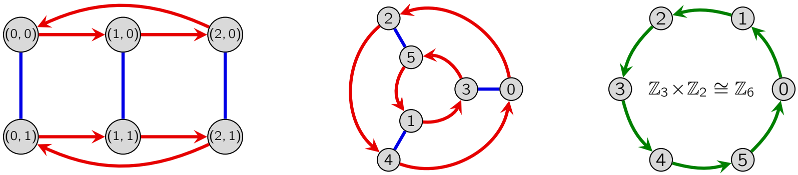
Definition

The direct product of groups A and B is the *set* $A \times B$, and the group operation is done component-wise: if $(a, b), (c, d) \in A \times B$, then

$$(a, b) * (c, d) = (ac, bd).$$

We call A and B the factors.

Sometimes, the direct product of cyclic groups is secretly cyclic.



Direct products of cyclic groups

Proposition

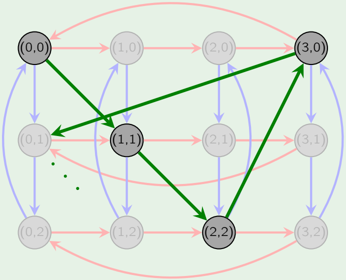
$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ if and only if $\gcd(n, m) = 1$.

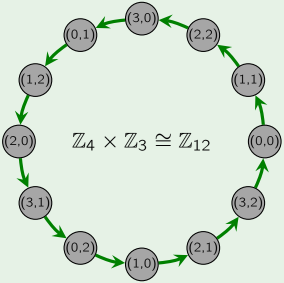
Proof

"$\Leftarrow$": 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, $k = \operatorname{lcm}(n, m) = nm$. ✓





Direct products of cyclic groups

Proposition

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

Proof (cont.)

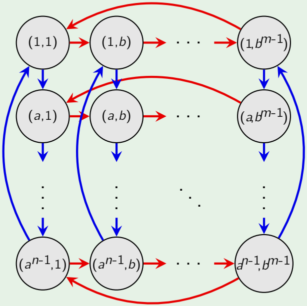
"$\Rightarrow$": Suppose $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$. Then $\mathbb{Z}_n \times \mathbb{Z}_m$ has an element (a, b) of order nm.

For convenience, we'll 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 graph 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 $\textbf{lcm}(n, m) = nm$. Therefore, $\textbf{gcd}(n, m) = 1$. $\square$

The fundamental theorem of finite abelian groups

Classification (two different versions)

Every finite abelian group A is isomorphic to a direct product of cyclic groups

$$A \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_m}, \qquad \text{for some } k_1, k_2, \dots, k_m \in \mathbb{N}, \text{ where}$$

- $k_i = p_i^{d_i}$, for a prime p_i and $d_i \in \mathbb{N}$, ("*prime powers*"), or
- k_i is a multiple of k_{i+1}, ("*elementary divisors*")

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

The classification theorem for *finitely generated* abelian groups 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:

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

Non-finitely generated abelian groups that we are familiar with include:

- The *rational numbers*, $\mathbb{Q}$, under addition
- The *real numbers*, $\mathbb{R}$, under addition
- The *complex numbers*, $\mathbb{C}$, under addition
- all of these (with 0 removed) under multiplication: $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$.
- the positive versions of these under multiplication: $\mathbb{Q}^+$, $\mathbb{R}^+$, and $\mathbb{C}^+$.

Permutation groups

Definition

Let X be a set. A permutation of X is a bijection $\pi \colon X \to X$.

The permutations of X form a group that we denote S_X. The special case when $X = \{1, \dots, n\}$ is the **symmetric group**, denoted S_n.

There are several notations for permutations, each with their strengths and weaknesses:

i	1	2	3	4	5	6
$\pi(i)$	2	3	1	6	5	4

"*one-line notation*"

"*permutation diagram*"

$$\pi = (1\,2\,3)\,(4\,6)$$

"*cycle notation*"

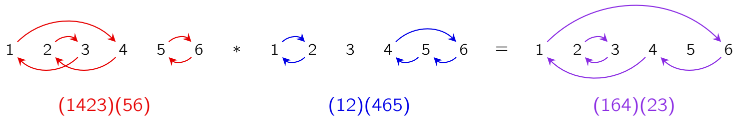
Notational convention

Composition of permutations will be done left-to-right. That is, given $\pi, \sigma \in S_n$,

$$\pi\sigma \quad \text{means "}\textit{do } \pi, \textit{ then do } \sigma\text{".}$$

Composing permutations in cycle notation

Let's practice composing two permutations:



Let's now do that in slow motion.

In the example above, we start with 1 and then read off:

- "**1** goes to 4, then 4 goes to 6"; Write: (1 6
- "6 goes to 5, then 5 goes to 4"; Write: (1 6 4
- "4 goes to 2, then 2 goes to **1**"; Write: (1 6 4), and start a new cycle.
- "**2** goes to 3, then 3 is fixed"; Write: (1 6 4) (2 3
- "3 goes to 1, then 1 goes to **2**"; Write: (1 6 4) (2 3), and start a new cycle.
- "**5** goes to 6, then 6 goes to **5**"; Write: (1 6 4) (2 3) (5); now we're done.

We typically omit 1-cycles (fixed points), so the permutation above is just (1 6 4) (2 3).

The symmetric group

Remark

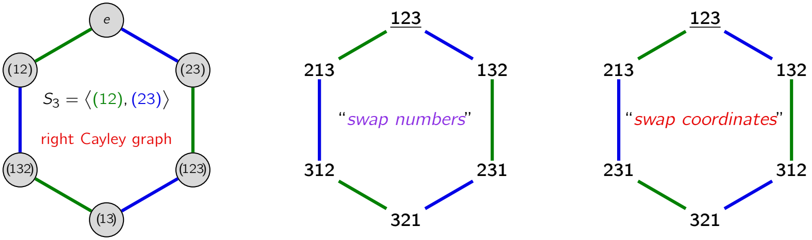
There are two canonical types of generating sets for S_n:

- Adjacent transpositions: $S_n = \langle (1\,2),\ (2\,3),\ \ldots,\ (n-1\ \ n) \rangle$.
- Any transposition and any n-cycle: $S_n = \langle (1\,2),\ \ (1\,2\,\cdots\,n{-}1\ \ n) \rangle$.

Instead of using configurations of the triangle, consider rearrangements of numbers:

$$\{\mathbf{123},\ \mathbf{132},\ \mathbf{213},\ \mathbf{231},\ \mathbf{312},\ \mathbf{321}\}.$$

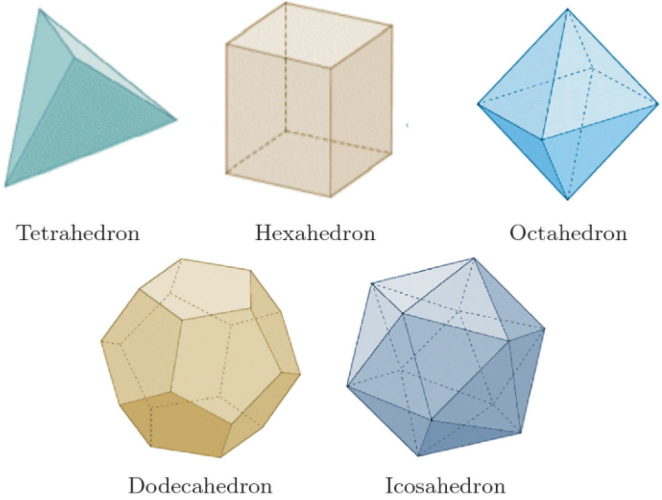
Clearly, S_3 canonically rearranges these configurations, but in two ways.



Later, we will understand this difference as a left group action vs. a right group action.

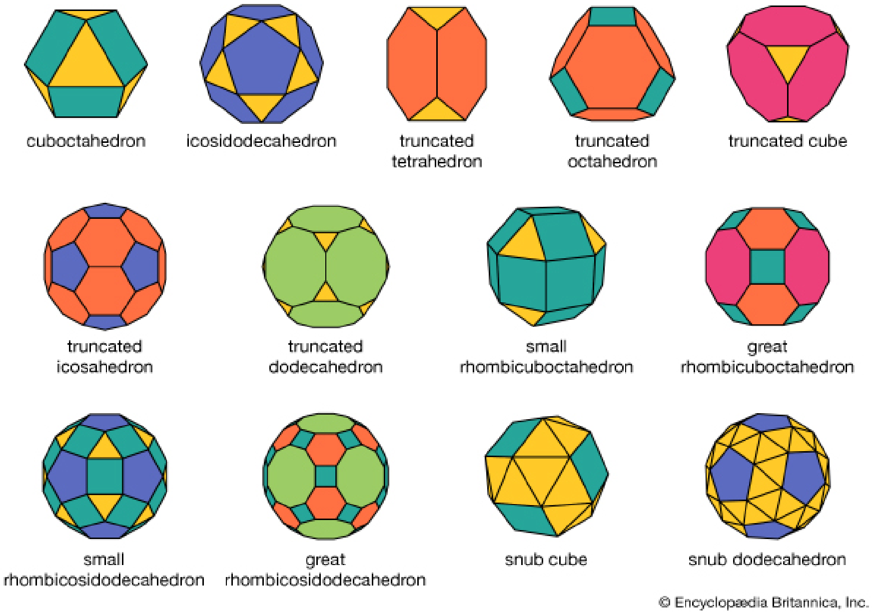
Platonic solids

There are exactly five regular polyhedra, called Platonic solids.



More general than the Platonic solids are the Archimedean solids.

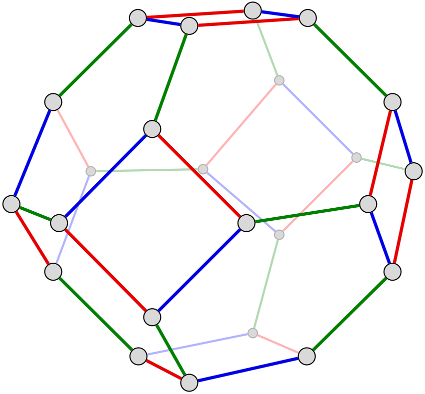
Archimedean solids



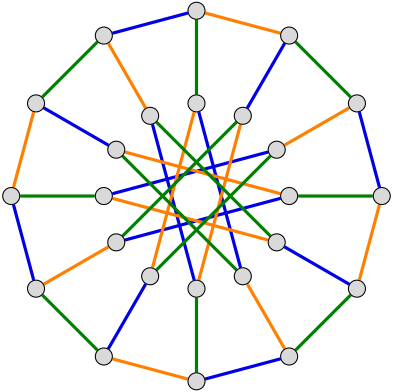
Archimedean solids and S_4

Below are Cayley graphs for the symmetric group

$$S_4 = \big\langle (12),\ (23),\ (34) \big\rangle = \big\langle (12), (13), (14) \big\rangle.$$



truncated octahedron; "*permutahedron*"



"*Nauru graph*"

Exercise: On the permutahedron, construct the Cayley graph for

$$S_4 = \big\langle (1\,2),\ (1\,2\,3\,4) \big\rangle.$$

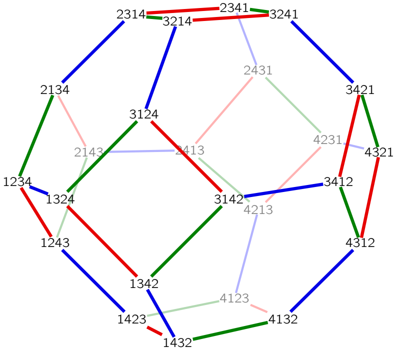
The left and right permutahedra

Definition

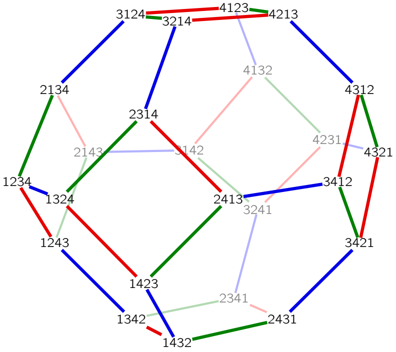
The (right) *n-permutahedron* is the convex hull of the $n!$ permutations of $(1, \dots, n) \in \mathbb{R}^n$.

This is an $(n-1)$-dimensional polytope, as it lies on the hyperplane $x_1 + \cdots + x_n = \frac{(n-1)n}{2}$.
It is also the (right) Cayley graph of

$$S_4 = \langle (12),\ (23),\ (34) \rangle.$$



"*swap coordinates*"



"*swap numbers*"

The alternating group

Definition / Proposition

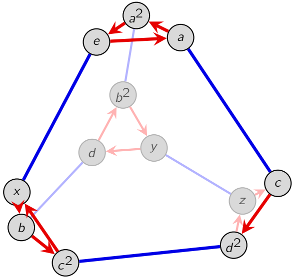
A permutation in S_n is either:

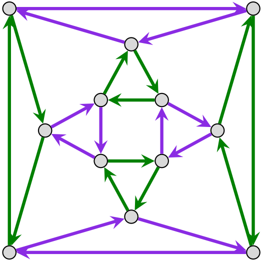
- even, if it can be written with an even number of transpositions, or
- odd, if it requires an odd number.

Definition

The set of even permutations in S_n is the **alternating group**, denoted A_n.

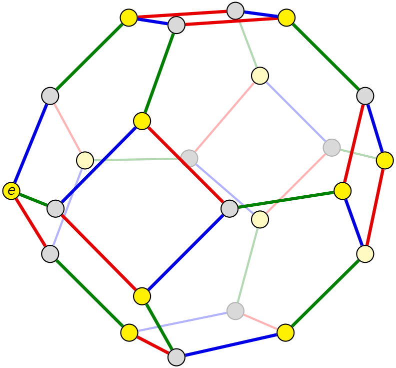
Here are Cayley graphs for A_4 on a truncated tetrahedron and cuboctahedron.



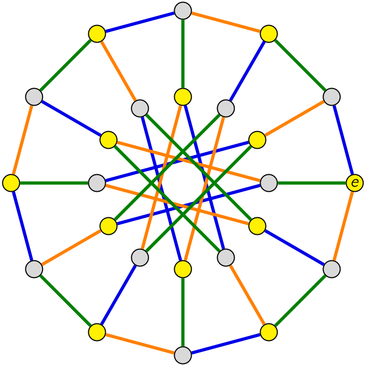


The appearance of A_4 in Cayley graphs for S_4

Let's highlight in yellow the even permutations in Cayley graphs for S_4.



$S_4 = \langle (12),\ (23),\ (34) \rangle$



$S_4 = \langle (12), (13), (14) \rangle$

Notice that any two paths between yellow nodes has **even length**.

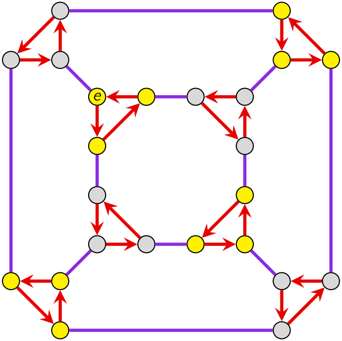
The appearance of A_4 in Cayley graphs for S_4

There are only five **cycle types** in S_4:

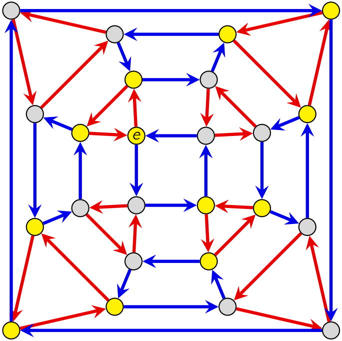
example element	e	(12)	(234)	(1234)	$(12)(34)$
parity	even	odd	even	odd	even
# elts	1	6	8	6	3

In both Cayley graphs, blue arrows flip the sign of the permutation; red arrows do not.

Once again, even permutations are highlighted in yellow.

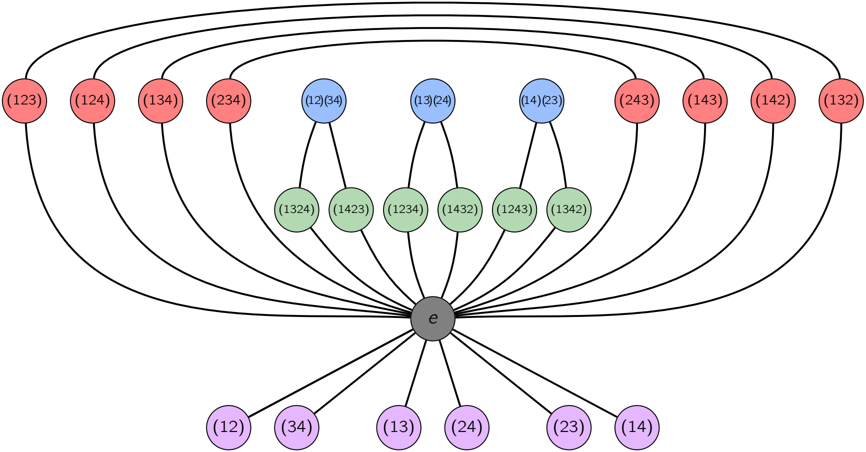


truncated cube



rhombicuboctahedron

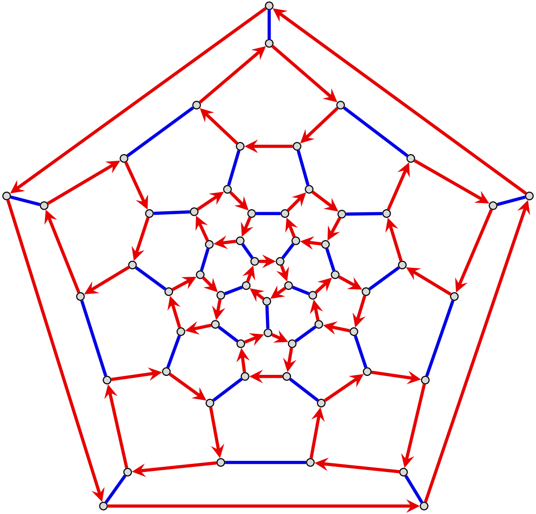
The cycle graph of S_4



A very important group

The group A_5 has special properties that we will learn about later.

Here is the Cayley graph of $A_5 = \langle (12345), (12)(34) \rangle$ on a truncated icosahedron.

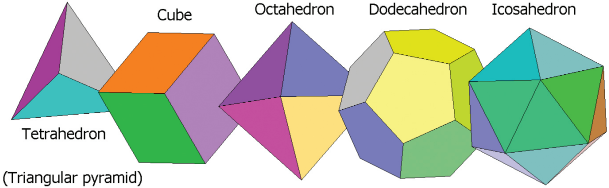


Symmetry groups of Platonic solids

Two-dimensional regular polytopes have rotation groups (C_n) and symmetry groups (D_n).

3D regular polytopes (Platonic solids) have these as well.

solid	**rotation group**	**symmetry group**
Tetrahedron	A_4	S_4
Cube	S_4	$S_4 \times C_2$
Octahedron	S_4	$S_4 \times C_2$
Icosahedron	A_5	$A_5 \times C_2$
Dodecahedron	A_5	$A_5 \times C_2$



There are higher-dimensional versions of the tetrahedron and cube, and their symmetry groups are S_n, and a group we haven't yet seen called $S_n \wr C_2$ (the "signed permutations").

Generalizing the quaternion group

The **quaternion group** Q_8 is generated by:

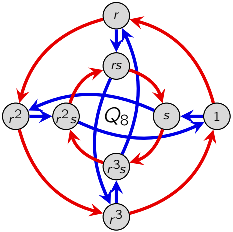
- a 4^{th} root of unity, $i = \zeta_4 = e^{2\pi i/4}$ ($2\pi/4$-rotation)
- the "imaginary number" j

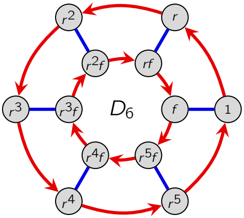
$$Q_8 = \langle i, j, k \rangle \cong \left\langle \underbrace{\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}}_{R=R_4}, \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{S}, \underbrace{\begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}}_{T=RS} \right\rangle.$$

The **dihedral group** is generated by

- an n^{th} root of unity, $r = \zeta_n = e^{2\pi i/n}$ ($2\pi/n$-rotation)
- a reflection f

$$D_n = \langle r, f \rangle \cong \left\langle \underbrace{\begin{bmatrix} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{bmatrix}}_{R_n}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{F} \right\rangle.$$



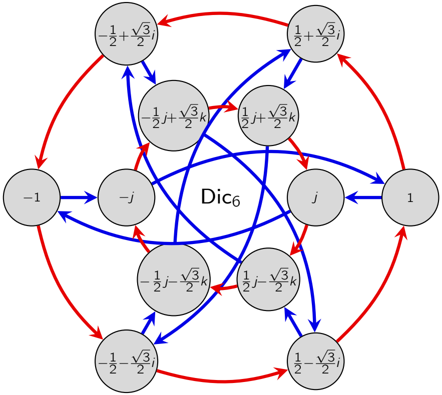


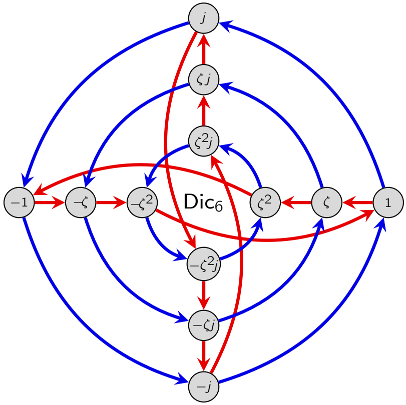
The dicyclic groups

Replacing $i \in Q_8$ with a larger (even) root of unity defines the **dicyclic group**:

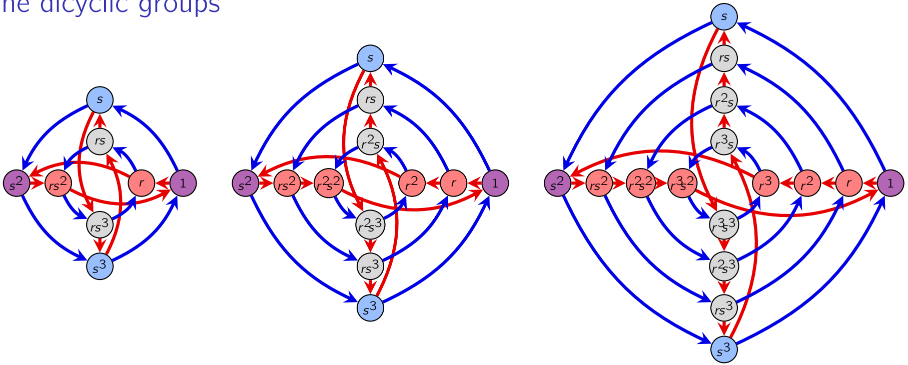
$$\mathrm{Dic}_n = \langle \zeta_n, j \rangle \cong \Bigg\langle \underbrace{\begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta_n} \end{bmatrix}}_{R=R_n}, \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{S} \Bigg\rangle \cong \langle r, s \mid r^n = s^4 = 1,\ r^{n/2} = s^2,\ rsr = s \rangle.$$

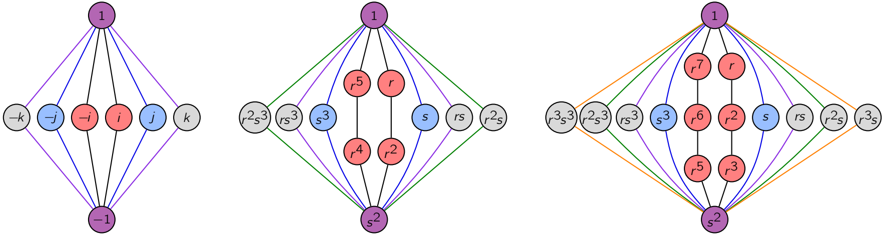
The multiplication rules $ij = k$ and $ji = -k$ remain unchanged.





The dicyclic groups

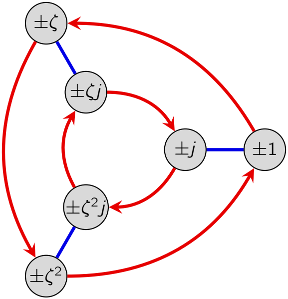




A quotient of the dicyclic group

Recall how we constructed a quotient of the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ that was isomorphic to V_4.

We can do a similar construction for dicyclic groups.



	± 1	$\pm\zeta$	$\pm\zeta^2$	$\pm j$	$\pm\zeta j$	$\pm\zeta^2 j$
± 1	± 1	$\pm\zeta$	$\pm\zeta^2$	$\pm j$	$\pm\zeta j$	$\pm\zeta^2 j$
$\pm\zeta$	$\pm\zeta$	$\pm\zeta^2$	± 1	$\pm\zeta j$	$\pm\zeta^2 j$	$\pm j$
$\pm\zeta^2$	$\pm\zeta^2$	± 1	$\pm\zeta$	$\pm\zeta^2 j$	$\pm j$	$\pm\zeta j$
$\pm j$	$\pm j$	$\pm\zeta^2 j$	$\pm\zeta j$	± 1	$\pm\zeta^2$	$\pm\zeta$
$\pm\zeta j$	$\pm\zeta j$	$\pm j$	$\pm\zeta^2 j$	$\pm\zeta$	± 1	$\pm\zeta^2$
$\pm\zeta^2 j$	$\pm\zeta^2 j$	$\pm\zeta j$	$\pm j$	$\pm\zeta^2$	$\pm\zeta$	± 1

The product $(\pm\zeta j) \cdot (\pm\zeta^2 j) = \pm\zeta^2$ means

"*the product of any element in* $\{\zeta j, -\zeta j\}$ *with any element in* $\{\zeta^2 j, -\zeta^2 j\}$ *is in* $\{\zeta^2, -\zeta^2\}$."

When $n = 2^m$, the dicyclic group $\mathrm{Dic}_{2^{n-1}}$ is called the generalized quaternion group, denoted Q_{2^n}.

The diquaternion group

Let's combine our representations of the quaternion and dihedral groups in a different way.

$$Q_8 = \langle i, j, k \rangle \cong \Bigg\langle \underbrace{\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}}_{R=R_4}, \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{S}, \underbrace{\begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}}_{T=RS} \Bigg\rangle, \qquad D_n = \langle r, f \rangle \cong \Bigg\langle \underbrace{\begin{bmatrix} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{bmatrix}}_{R_n}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{F} \Bigg\rangle.$$

Consider the group generated by adding the reflection matrix from D_n to Q_8.

This is the Pauli group on 1 qubit. We will call it the diquaternion group

$$\mathrm{DQ}_8 = \langle X, Y, Z \rangle = \{ \pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ \},$$

generated by the Pauli matrices from quantum mechanics and information theory:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

It is easy to check that

$$XY = R \quad \text{“}i\text{”}, \qquad XZ = S \quad \text{“}j\text{”}, \qquad YZ = \overline{T} \quad \text{“}k\text{”}.$$

This group can be constructed in other ways as well:

- as a semidirect product, $Q_8 \rtimes_2 C_2$, and $D_4 \rtimes_2 C_2$, and $(C_4 \rtimes C_2) \rtimes_3 C_2$.
- as the "central product" $\mathrm{DQ}_8 = C_4 \circ D_4$.

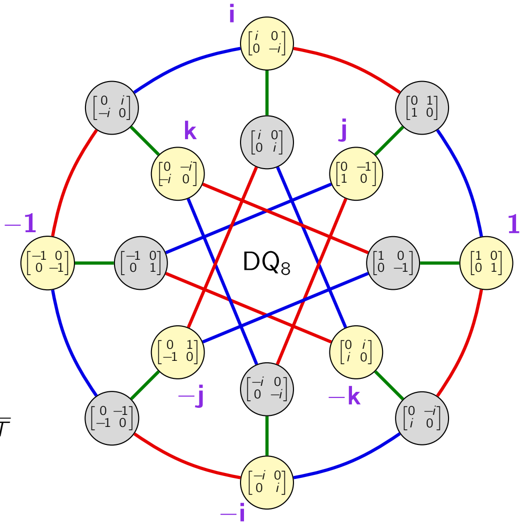
The diquaternion group

$$X = F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

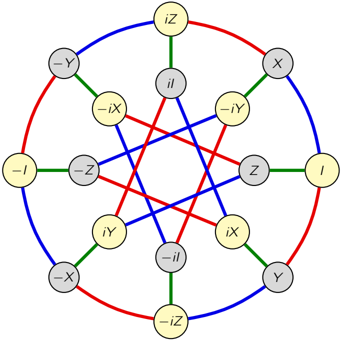
$$XY = R, \quad XZ = S, \quad YZ = \overline{T}$$

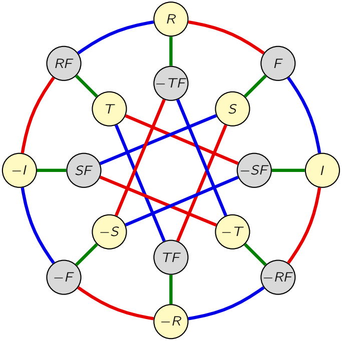


The diquaternion group

The diquaternion group is usually generated with Pauli matrices, $\mathrm{DQ}_8 = \langle X, Y, Z \rangle$.

We can also write it as $\mathrm{DQ}_8 = \langle R, S, T, F \rangle$ where $Q_8 = \langle R, S, T \rangle$ and $D_n = \langle R_n, F \rangle$.



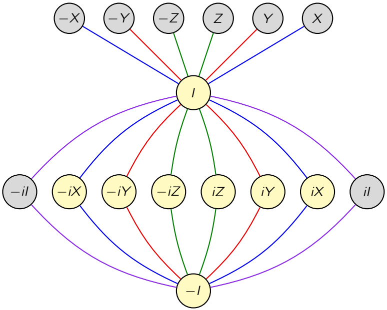


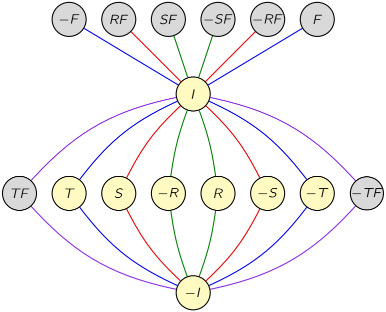
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad R = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \; S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \; T = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

The diquaternion group

Here are two cycle graphs for

$$\mathrm{DQ}_8 = \big\langle X, Y, Z \big\rangle = \langle R, S, T, F \rangle.$$





$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad R = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \; S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \; T = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

Do you see a way to generalize this further? What if we use a different root of unity?

Generalized diquaternion groups

Replace $i = \zeta_4 = e^{2\pi i/4}$ with $\zeta_n = e^{2\pi i/n}$ to get the generalized diquaternion group

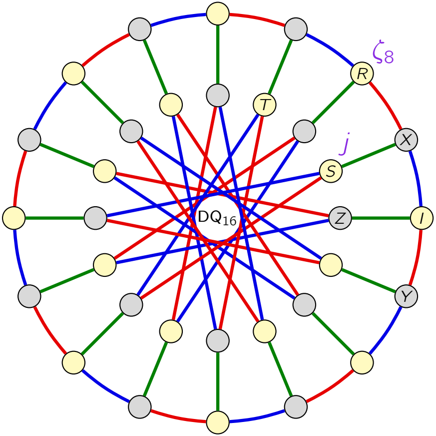
$$\mathrm{DQ}_n := \langle \zeta_n, j, \zeta_n j, f \rangle \cong \Big\langle \underbrace{\begin{bmatrix} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{bmatrix}}_{R=R_n}, \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{S}, \underbrace{\begin{bmatrix} 0 & -\zeta_n \\ \bar{\zeta}_n & 0 \end{bmatrix}}_{T=T_n}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{F} \Big\rangle \cong \mathrm{Dic}_n \rtimes_\theta C_2.$$

$$X = F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y := Y_8 = \begin{bmatrix} 0 & \bar{\zeta}_8 \\ \zeta_8 & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

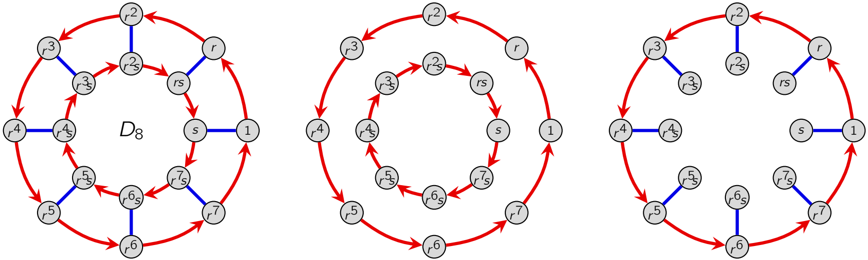
$$XY_8 = R_8, \qquad XZ = S, \qquad Y_8 Z = \overline{T}_8$$



Generalizing the dihedral groups

The dicyclic groups describe one way to started with a Cayley graph of $D_n = \langle r, f \rangle$, remove the blue arcs, and re-wire them.

What if we kept those, but re-wired the inner length-n red cycle?



In other words, we want to construct a group G that

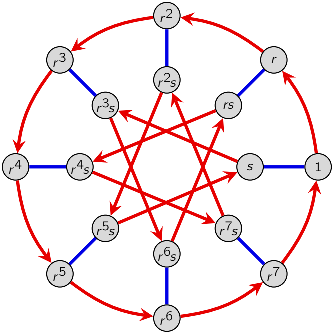
- has an element r of order n
- has an element $s \notin \langle r \rangle$ of order 2.

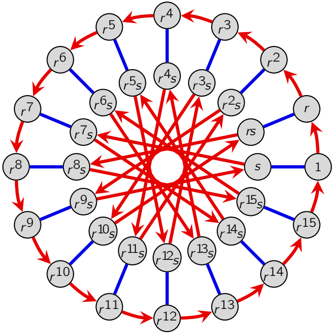
Equivalently, what can we replace the relation $srs = r^{n-1}$ with? That is,

$$G = \big\langle r, s \mid r^n = 1,\ s^2 = 1,\ ??? \big\rangle.$$

Semidihedral groups

If n is a power of 2, we can replace $srs = r^{n-1}$ with $srs = r^{n/2-1}$.





Definition

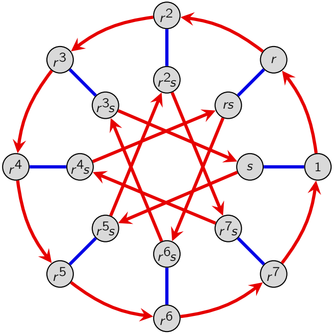
For each power of two, the semidihedral group of order 2^n is defined by

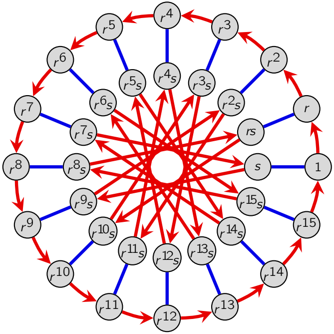
$$\mathrm{SD}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs = r^{2^{n-2}-1} \rangle.$$

Do you see another way we can re-wire these inner red arrows?

Semiabelian groups

Still assuming n is a power of 2, let's replace $srs = r^{n/2-1}$ with $srs = r^{n/2+1}$.





Definition

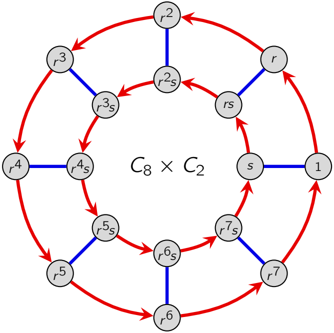
For each power of two, the semiabelian group of order 2^n is defined by

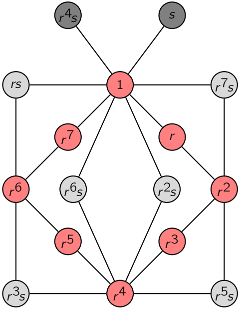
$$\mathrm{SA}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs = r^{2^{n-2}+1} \rangle.$$

One more re-wiring

Of course, there's one more way that we can re-wire the dihedral group...

Here is its Cayley graph and cycle graph.





When this group has order 2^n, its presentation is

$$C_{2^n-1} \times C_2 = \left\langle r, s \mid r^{2^{n-1}} = s^2 = 1, \; srs = r \right\rangle.$$

Remarkably, this and the other three we've seen are the *only* possibilities:

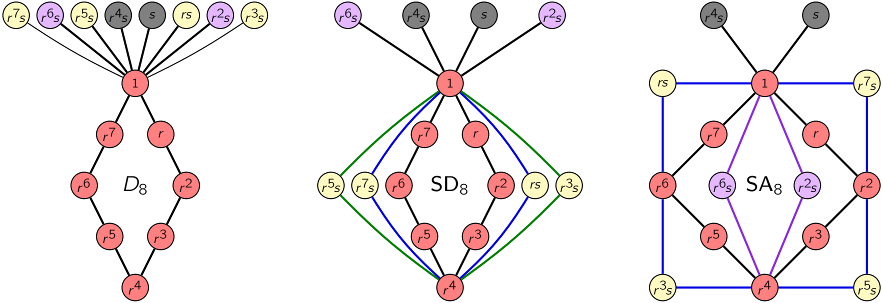
$srs = r^{-1}$ (dihedral), $\quad srs = r^{2^{n-2}-1}$ (semidihedral), $\quad srs = r^{2^{n-2}+1}$ (semiabelian).

Dihedral vs. semidiheral vs. semiabelian groups

In other words, there are exactly 4 groups of order 2^n with both:

- an element r of order 2^{n-1}
- an element $s \notin \langle r \rangle$ of order 2.

Let's compare the cycle graphs of the three non-abelian groups from this list:



Remark

The semiabelian group SA_n and the abelian group $C_n \times C_2$ have the same orbit structure!

This surprising fact has profound consequences that we'll see when we study subgroups.

Dihedral vs. semidiheral vs. semiabelian groups

Recall our canonical representations of the cyclic and dihedral groups

$$C_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix} \right\rangle, \qquad D_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle, \qquad \zeta_n = e^{2\pi i/n}.$$

When n is even, the dicyclic groups are represented by

$$\mathrm{Dic}_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle.$$

When $n = 2^m$, this is also called the generalized quaternion group, denoted Q_{2^m}.

In this case, we also get a semidihedral and a semiabelian group:

$$\mathrm{SD}_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & -\overline{\zeta}_n \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle, \qquad \mathrm{SA}_n \cong \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & -\zeta_n \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle.$$

Note that for *any* $n \in \mathbb{N}$, the matrices above generate *some* group.

Exploratory question

What groups do the above representations give if, e.g., n is odd, or not a power of 2?

Non-abelian groups of order 2^n

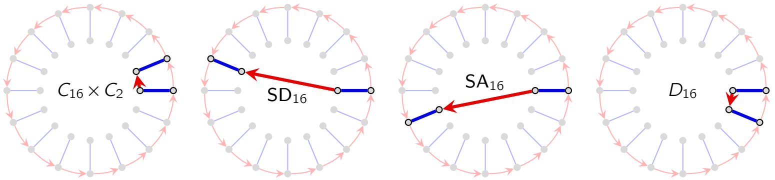
Theorem

There are exactly six groups of order 2^n that have an element r of order 2^{n-1}:

1. The **cyclic group** $C_{2^n} = \langle r, \mid r^{2^n} = 1 \rangle$.
2. The **abelian group** $C_{2^{n-1}} \times C_2 = \langle r, s \mid, \mid r^{2^{n-1}} = s^2 = 1 \rangle$.
3. The **dihedral group** $D_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs = r^{-1} \rangle$.
4. The dicyclic group $\mathrm{Dic}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^4 = 1,\ r^{2^{n-2}} = s^2,\ rsr = s \rangle$.
5. The semidihedral group $\mathrm{SD}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs = r^{2^{n-2}-1} \rangle$.
6. The semiabelian group $\mathrm{SA}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs = r^{2^{n-2}+1} \rangle$.

As we did before, we can ask:

what groups do these presentations describe when $2n$ is not a power of 2?



Groups of matrices

Matrices are a rich source of groups in their own right.

Definition

A ring is an abelian group R that is additionally

- closed under multiplication, and
- satisfies the distributive property.

If we can also divide by any nonzero element, it is a field, $\mathbb{F}$.

Definition

Let $\text{Mat}_n(\mathbb{F})$ be the set of $n \times n$ matrices with coefficients from $\mathbb{F}$.

The general linear group of degree n over R is the set of invertible matrices with coefficients from R:

$$\text{GL}_n(R) = \{A \in \text{Mat}_n(R) \mid \det A \neq 0\}.$$

The special linear group is the subgroup of matrices with determinant 1:

$$\text{SL}_n(R) = \{A \in \text{GL}_n(R) \mid \det A = 1\}.$$

An interesting group of order 24

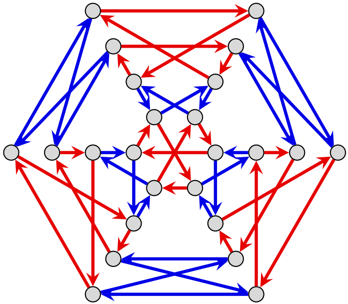
Some interesting finite groups arise as special or general linear groups over $\mathbb{Z}_q$. For example,

$$\mathsf{SL}_2(\mathbb{Z}_3) = \langle A, B \mid A^3 = B^3 = (AB)^2 \rangle = \langle A, B, C \mid A^3 = B^3 = C^2 = CAB \rangle \cong Q_8 \rtimes \mathbb{Z}_3,$$

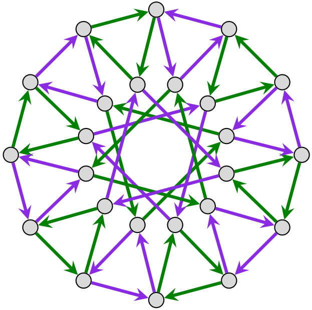
and the matrices A and B can be taken to be

$$A = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}, \qquad B = \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 1 & -1 \end{bmatrix}.$$

Here's are Cayley graphs for different generating sets:



$\langle R, S \mid R^6 = S^4 = (RS)^3 = I \rangle$



$\langle a, b \mid a^3 = b^3 = (ab)^3 \rangle$

The Hamiltonians

The group $\mathrm{SL}_2(\mathbb{Z}_3)$ can be represented with quaternions. The Hamiltonians are the ring

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

One way to represent these is with 2×2 matrices over $\mathbb{C}$:

$$\mathbb{H} \cong \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} : z, w \in \mathbb{C} \right\} = \left\{ \begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

Yet another way involves 4×4 matrices over $\mathbb{R}$:

$$\mathbb{H} \cong \left\{ \begin{bmatrix} a & b & -d & -c \\ -b & a & -c & d \\ d & c & a & b \\ c & -d & -b & a \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

Removing 0 from $\mathbb{H}$ defines a multiplicative group $\mathbb{H}^*$ with lots of interesting subgroups.

One of them is the unit quaternions, which physicists assoiciate with points in a 3-sphere:

$$S^3 := \{a + bi + cj + dk \mid a^2 + b^2 + c^2 + d^2 = 1\}.$$

The group $\mathrm{SL}_2(\mathbb{Z}_3)$ is isomorphic to a subgroup called the binary tetrahedral group,

$$\mathrm{SL}_2(\mathbb{Z}_3) \cong 2\mathrm{T} := \{\pm 1, \pm i, \pm j, \pm k, \tfrac{1}{2}(\pm 1 \pm i \pm j \pm k)\} \leq S^3.$$

Matrix groups over other finite fields

The group $\mathsf{GL}_n(\mathbb{Z}_p)$ consists of the linear maps of the vector space $\mathbb{Z}_p^n$ to itself.

Each one is determined by an ordered basis $v_1, \dots, v_n$ of $\mathbb{Z}_p^n$.

Let's count these. There are:

1. $p^n - 1$ choices for v_1, then
2. $p^n - p$ choices for v_2, then
3. $p^n - p^2$ choices for v_3, and so on...

n. $p^n - p^{n-1}$ choices for v_n.

Therefore,

$$\big|\,\mathsf{GL}_n(\mathbb{Z}_p)\big| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}).$$

These groups have many subgroups, and they often happen to coincide with familiar groups that we have seen.

For example, by "dumb luck",

$$D_9 \cong \left\langle \begin{bmatrix} 16 & 10 \\ 7 & 14 \end{bmatrix}, \begin{bmatrix} 14 & 6 \\ 10 & 3 \end{bmatrix} \right\rangle \leq \mathsf{GL}_2(\mathbb{Z}_{17}), \qquad \mathsf{Dic}_{12} \cong \left\langle \begin{bmatrix} 2 & 7 \\ 7 & 3 \end{bmatrix}, \begin{bmatrix} 0 & 10 \\ 1 & 0 \end{bmatrix} \right\rangle \leq \mathsf{GL}_2(\mathbb{Z}_{11}).$$

Affine groups

Let V be a vector space over a $\mathbb{F}$. A map $L\colon V \to V$ is linear if

$$L(c\mathbf{x} + d\mathbf{y}) = cL\mathbf{x} + dL\mathbf{y}, \qquad \text{for all } x, y \in V \text{ and } c, d \in \mathbb{F}.$$

If $\dim V = n < \infty$, we can write this with an $n \times n$ matrix.

Key point

- A linear map $f\colon V \to V$ has the form $f(\mathbf{x}) = A\mathbf{x}$.
- An affine map $f\colon V \to V$ has the form $f(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$.

The 1-dimensional general affine group over a field $\mathbb{F}$ as

$$\mathrm{AGL}_1(\mathbb{F}) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{F},\ a \neq 0 \right\}.$$

The 2-dimensional general affine group can be defined as

$$\mathrm{AGL}_2(\mathbb{F}) = \left\{ \begin{bmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ 0 & 0 & 1 \end{bmatrix} : a_{ij}, b_j \in \mathbb{F},\ a_{11}a_{22} - a_{12}a_{21} \neq 0 \right\}.$$

We can encode an affine map of an n-dimensional space V as an $(n+1) \times (n+1)$ matrix:

$$\mathbf{y} = f(\mathbf{x}) = A\mathbf{x} + \mathbf{b}, \qquad \text{as} \qquad \begin{bmatrix} \mathbf{y} \\ 1 \end{bmatrix} = \begin{bmatrix} A & \mathbf{b} \\ \mathbf{0} & 1 \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ 1 \end{bmatrix}$$

Other finite groups

The complete classification of finite groups is an impossible task.

However, work along these lines is worthwhile, because much can be learned from studying the structure of groups.

Open-ended question

What group structural properties are possible, what are impossible, and how does this depend on $|G|$?

One approach is to first understand basic "building block groups," and then deduce properties of larger groups from these building blocks, and how to put them together.

In chemistry, "building blocks" are atoms. In number theory, they are prime numbers.

What is a group theoretic analogue of this?

There are several possible answers.

One approach is to study groups that cannot be collapsed by a nontrivial quotient. These are called simple.

The classification of finite simple groups was completed in 2004. It took over 10000 pages of mathematics spread over 500 papers and 50+ years.

p-groups

A different approach to classify groups is to motivated by the following:

> *to understand groups of order $72 = 2^3 \cdot 3^2$, it would be helpful to first understand groups of order $2^3 = 8$ and $3^2 = 9$.*

Definition

If p is prime, then a p-group is any group G of order p^n.

Let's look at small powers of p.

Every group of order p is cyclic, and hence abelian. We can ask:

For what other integers n do there not exist any nonabelian groups?

We don't yet have the tools to answer this. But let's investigate for small powers of p:

Groups of order p^2.

- There are only two: $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.

Groups of order p^3. Staring with $p = 2$:

- three are abelian: $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, and $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$
- the dihedral group D_4
- the quaternion group Q_8.

Theorem

For each prime p, there are 5 groups of order p^3.

Surprisingly, the pattern for $p=2$ does not generalize.

Groups of order p^3, for $p>2$

- the Heisenberg group over $\mathbb{Z}_p$,

$$\operatorname{Heis}(\mathbb{Z}_p) := \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{Z}_p \right\} \cong C_p^2 \rtimes C_p,$$

- another group defined as

$$G_p := \left\{ \begin{bmatrix} 1+pm & b \\ 0 & 1 \end{bmatrix} : m, b \in \mathbb{Z}_{p^2} \right\} \cong C_{p^2} \rtimes C_p.$$

These generalize from p^3 to p^{1+2n}, and are called extraspecial p-groups:

$$M(p) = \langle a, b, c \mid a^p = b^p = c^p = (ab)^2 = (ac)^2 = 1,\ ab = abc \rangle,$$
$$N(p) = \langle a, b, c \mid a^p = b^p = c,\ (ab)^2 = (ac)^2 = 1,\ ab = abc \rangle.$$

Groups of order ≤ 30

order	groups	order	groups	order	groups	order	groups
1	C_1	12 (cont.)	A_4	18 (cont.)	$D_3 \times C_2$	24 (cont.)	$Q_8 \times C_3$
2	C_2	13	C_{13}		$C_3 \rtimes D_3$		$D_3 \times C_4$
3	C_3	14	C_{14}	19	C_{19}		$D_3 \times C_2^2$
4	C_4		D_7	20	C_{20}		$C_3 \rtimes C_8$
	C_2^2	15	C_{15}		$C_{10} \times C_2$		$C_3 \rtimes D_4$
5	C_5	16	C_{16}		D_{10}	25	C_{25}
6	C_6		$C_8 \times C_2$		Dic_{10}		$C_5 \times C_5$
	D_3		C_4^2		$\mathrm{AGL}_1(\mathbb{Z}_5)$	26	C_{26}
7	C_7		$C_4 \times C_2^2$	21	C_{21}		D_{13}
8	C_8		C_2^4		$C_7 \rtimes C_3$	27	C_{27}
	$C_4 \times C_2$		D_8	22	C_{22}		$C_9 \times C_3$
	C_2^3		SD_8		D_{22}		C_3^3
	D_4		SA_8	23	C_{23}		$C_9 \rtimes C_3$
	Q_8		Q_{16}	24	C_{24}		$C_3^2 \rtimes C_3$
9	C_9		$D_4 \times C_2$		$C_{12} \times C_2$	28	C_{28}
	$C_3 \times C_3$		$Q_8 \times C_2$		$C_6 \times C_2^2$		$C_{14} \times C_2$
10	C_{10}		$C_4 \rtimes C_4$		D_{12}		D_{14}
	$C_5 \times C_2$		$C_2^2 \rtimes C_4$		Dic_{12}		Dic_{14}
11	C_{11}		DQ_8		S_4	29	C_{29}
12	C_{12}	17	C_{17}		$\mathrm{SL}_2(\mathbb{Z}_3)$	30	C_{30}
	$C_6 \times C_2$	18	C_{18}		$A_4 \times C_2$		D_{15}
	D_6		$C_6 \times C_3$		$\mathrm{Dic}_{12} \times C_2$		$D_5 \times C_3$
	Dic_6		D_9		$D_4 \times C_3$		$D_3 \times C_5$