

## Chapter 2: Examples of groups

Matthew Macauley

Department of Mathematical Sciences  
Clemson University

<http://www.math.clemson.edu/~macaule/>

Math 4120, Modern Algebra

## Families of groups

In the previous chapter, we encountered a handful of groups that were meant to appeal to intuition and motivate key concepts.

In this chapter, we will 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.

We'll show that *every* finite group is isomorphic to a permutation group.

Then, by rewiring the Cayley diagrams of dihedral groups, we'll encounter:

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

Finally, we'll take a tour of:

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

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

## A few basic definitions

We'll study subgroups in Chapter 3, but it's helpful to formally define this concept now.

### Definition

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

### Definition

The **order of a group**  $G$  is its size as a set, denoted by  $|G|$ .

### Definition

The **order of an element**  $g \in G$  is  $|g| := |\langle g \rangle|$ , i.e., either

- the minimal  $k \geq 1$  such that  $g^k = e$ , or
- $\infty$ , if there is no such  $k$ .

## A few basic definitions

The complex numbers are the set

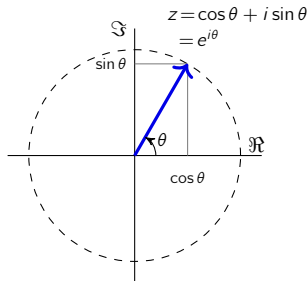
$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}, \quad \text{where } i^2 = -1.$$

By **Euler's identity**,  $e^{i\theta} = \cos \theta + i \sin \theta$  lies on the unit circle.

From this, we get the **polar form**:

$$z = a + bi = Re^{i\theta}, \quad \tan \theta = b/a.$$

The **norm** of  $z \in \mathbb{C}$  is  $|z| := R = \sqrt{a^2 + b^2}$ .

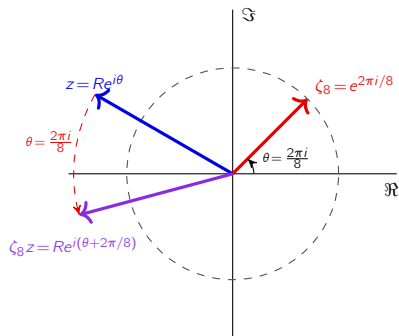
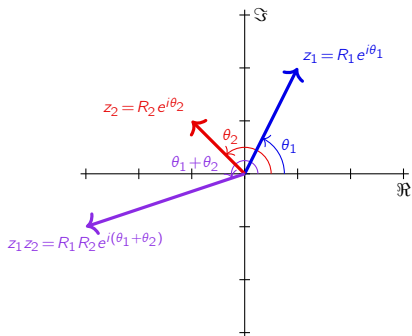


### Remark

If two complex numbers are multiplied, their **lengths multiply** and their **angles add**.

$$z_1 = R_1 e^{i\theta_1}, \quad z_2 = R_2 e^{i\theta_2} \quad \implies \quad z_1 z_2 = (R_1 e^{i\theta_1})(R_2 e^{i\theta_2}) = R_1 R_2 e^{i(\theta_1 + \theta_2)}.$$

# Review of complex numbers



The **complex conjugate** of  $z = Re^{i\theta} = a + bi$  is

$$\bar{z} = Re^{-i\theta} = a - bi,$$

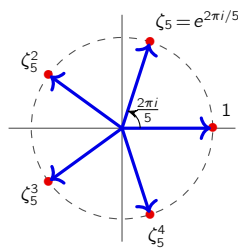
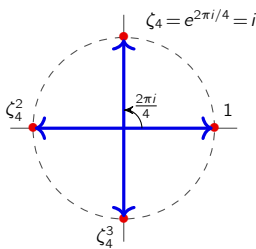
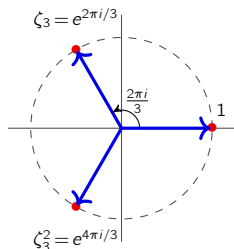
which is the reflection of  $z$  across the real axis.

Note that

$$|z|^2 = z \cdot \bar{z} = Re^{i\theta} Re^{-i\theta} = R^2 e^0 = R^2 \implies |z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2} = R.$$

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

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

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

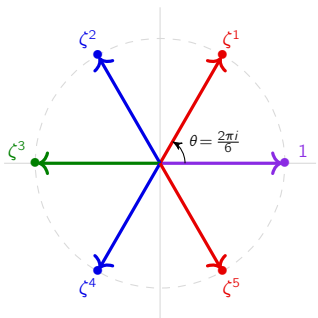
### Remark

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

## A motivating example: the 6<sup>th</sup> roots of unity

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

*Do you see how this generalizes for arbitrary  $n$ ?*

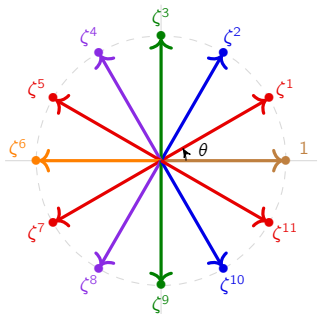
# Cyclotomic polynomials

The  $n^{\text{th}}$  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  $n^{\text{th}}$  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<sup>th</sup> roots of unity:  $\zeta^1, \zeta^5, \zeta^7, \zeta^{11}$
- primitive 6<sup>th</sup> roots of unity:  $\zeta^2, \zeta^{10}$
- primitive 4<sup>th</sup> roots of unity:  $\zeta^3, \zeta^9$
- primitive 3<sup>rd</sup> roots of unity:  $\zeta^4, \zeta^8$
- primitive 2<sup>nd</sup> root of unity:  $\zeta^6$
- primitive 1<sup>st</sup> root of unity:  $\zeta^0 = 1$ .

## Remark

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



## Reflection matrices

The roots of unity are convenient for representing rotations, but not reflections.

A  $2 \times 2$  real-valued matrix  $A$  is a **linear transformation**

$$A: \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}.$$

A reflection across the  $x$ -axis (i.e.,  $v \in V_4$ ) is the map  $(x, y) \mapsto (x, -y)$ .

A reflection across the  $y$ -axis (i.e.,  $h \in V_4$ ) is the map  $(x, y) \mapsto (-x, y)$ .

In matrix form, these are

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -y \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -x \\ y \end{bmatrix}.$$

Multiplying these matrices in either order is  $-I$ , which is the map  $(x, y) \mapsto (-x, -y)$ :

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -x \\ -y \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Mathematically, this is a **representation** of the group  $V_4$ :

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

## Rotation matrices

For  $\theta \in [0, 2\pi)$ , the **rotation matrix**

$$A_\theta = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

is a counterclockwise rotation of  $\mathbb{R}^2$  about the origin by  $\theta$ .

Rotating by  $\theta_1$  and then by  $\theta_2$  is a rotation by  $\theta_1 + \theta_2$ . Algebraically,

$$A_{\theta_1} A_{\theta_2} = A_{\theta_1 + \theta_2}.$$

Recall that multiplication by  $e^{2\pi i/n}$  is a counterclockwise rotation of  $2\pi/n$  radians in  $\mathbb{C}$ .

In terms of matrices, this is multiplication by

$$A_{2\pi/n} = \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix}.$$

We can also represent rotations with complex matrices:

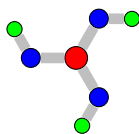
$$R_n := \begin{bmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{bmatrix} = \begin{bmatrix} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{bmatrix}.$$

# Cyclic groups

## Definition

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

Finite cyclic groups describe the symmetries of objects that have *only* rotational symmetry.



We have seen three ways to represent cyclic groups.

1. By **roots of unity**:

$$C_n \cong \langle \zeta_n \rangle = \langle e^{2\pi i/n} \rangle = \{ e^{2\pi i k/n} \mid k = 0, \dots, n-1 \} \subseteq \mathbb{C}.$$

2. By **real rotation matrices**:

$$C_n \cong \langle A_{2\pi/n} \rangle = \left\langle \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix} \right\rangle.$$

3. By **complex rotation matrices**:

$$C_n \cong \langle R_n \rangle = \left\langle \begin{bmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{bmatrix} \right\rangle = \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{bmatrix} \right\rangle.$$

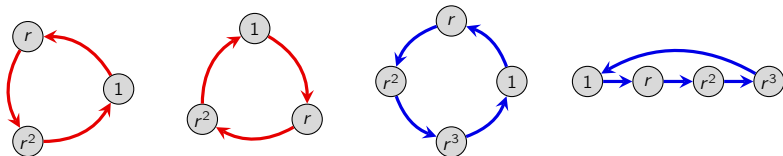
## Cyclic groups, multiplicatively

### Definition

For  $n \geq 1$ , the **multiplicative cyclic group**  $C_n$  is the set

$$C_n = \{1, r, r^2, \dots, r^{n-1}\},$$

where  $r^i r^j = r^{i+j}$ , and the exponents are taken modulo  $n$ . The identity is  $r^0 = r^n = 1$ .



It is clear that a presentation for this is

$$C_n = \langle r \mid r^n = 1 \rangle.$$

Note that  $r^2$  generates  $C_5$ :

$$(r^2)^0 = 1, \quad (r^2)^1 = r^2, \quad (r^2)^2 = r^4, \quad (r^2)^3 = r^6 = r, \quad (r^2)^4 = r^8 = r^3.$$

Do you have a conjecture about for which  $k$  does  $C_n = \langle r^k \rangle$ ?

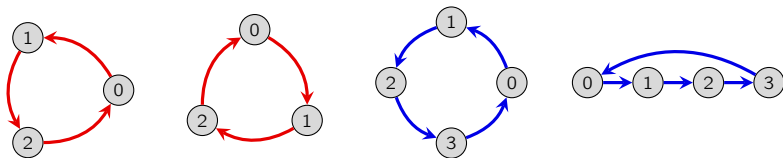
# Cyclic groups, additively

## Definition

For  $n \geq 1$ , the **additive cyclic group**  $\mathbb{Z}_n$  is the set

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\},$$

where the binary operation is **addition modulo  $n$** . The identity is 0.



We can write a group presentation additively:

$$\mathbb{Z}_n = \langle 1 \mid n \cdot 1 = 0 \rangle.$$

Note that 2 generates  $\mathbb{Z}_5$ :

$$0 \cdot 2 = 0, \quad 1 \cdot 2 = 2, \quad 2 \cdot 2 = 4, \quad 2 \cdot 3 = 6 \equiv_5 1, \quad 2 \cdot 4 = 8 \equiv_5 3.$$

## Remark

It is wrong to write  $C_n = \mathbb{Z}_n$ ; instead, we say  $C_n \cong \mathbb{Z}_n$ .

## Generators of cyclic groups

Recall that the **greatest common divisor** of nonzero  $a, b \in \mathbb{Z}$  is

$$\gcd(a, b) = \min \{|ax + by| : x, y \in \mathbb{Z}\},$$

and they are **co-prime** if  $\gcd(a, b) = 1$ .

### Proposition

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

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

### Proof

“ $\Leftarrow$ ”: We need to show that  $1 \in \langle k \rangle$ .

In other words, that  $1 \equiv_n ky$  for some  $y \in \mathbb{Z}$ .

If  $\gcd(n, k) = 1$ , then write  $1 = nx + ky$  for some  $x, y \in \mathbb{Z}$ . Taking this modulo  $n$  yields

$$1 \equiv_n nx + ky \equiv_n ky.$$

We'll leave the “ $\Rightarrow$ ” direction as an exercise. □

## Cayley tables of cyclic groups

Modular addition has a nice visual appearance in the Cayley tables for cyclic groups, if we order the elements  $0, 1, \dots, n - 1$ .

Here are two different ways to write the Cayley table for  $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ .

|   | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

|   | 0 | 1 | 3 | 2 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 3 | 2 | 4 |
| 1 | 1 | 2 | 4 | 3 | 0 |
| 3 | 3 | 4 | 1 | 0 | 2 |
| 2 | 2 | 3 | 0 | 4 | 1 |
| 4 | 4 | 0 | 2 | 1 | 3 |

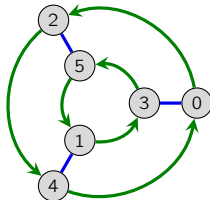
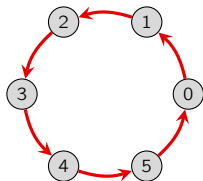
The second Cayley table was one of our mystery Latin square from the previous chapter.

## Minimal vs. minimum generating sets

There are many ways to generate the cyclic group of order 6:

$$\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle = \langle 2, 3 \rangle = \langle 3, 4 \rangle = \langle 1, 2 \rangle = \langle 1, 2, 3 \rangle = \dots$$

The following Cayley diagrams illustrate two of these.



### 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  $|S| \leq |T|$ .

Finite groups always have at least one minimum generating set.

*What about infinite groups?*



# Infinite cyclic groups

## Definition

The **additive infinite cyclic group** is

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

the integers under addition. The **multiplicative infinite cyclic group** is

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

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  $\mathbb{Z} = \langle 2, 3 \rangle$ :



# Orbits

## Definition

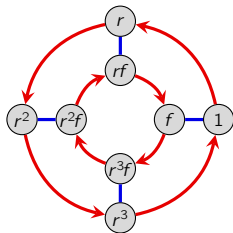
The **orbit** of an element  $g \in G$  is the **cyclic subgroup**

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

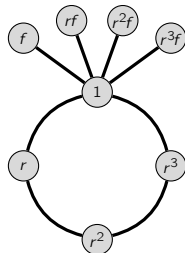
and its **order** is  $|g| := |\langle g \rangle|$ .

We can visualize the orbits by the (undirected) **orbit graph**, or **cycle graph**.

This is best seen by an example:



| element | orbit            |
|---------|------------------|
| 1       | {1}              |
| r       | {1, r, r^2, r^3} |
| r^2     | {1, r^2}         |
| r^3     | {1, r, r^2, r^3} |
| f       | {1, f}           |
| rf      | {1, rf}          |
| r^2f    | {1, r^2f}        |
| r^3f    | {1, r^3f}        |



By convention, we typically only draw **maximal orbits**.

# Abelian groups

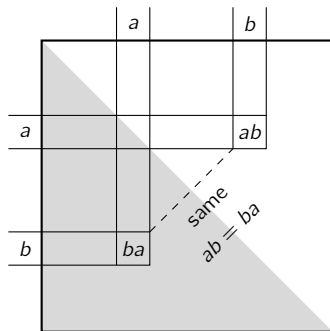
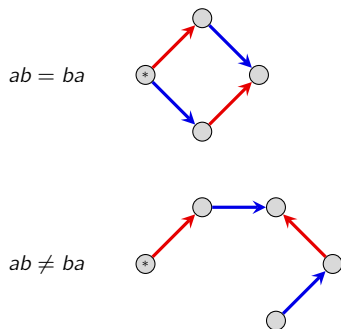
## Definition

A group  $G$  is **abelian** if  $ab = ba$  for all  $a, b \in G$ .

## Remark

To check that  $G$  is abelian, it suffices to only check that  $ab = ba$  for all pairs of **generators**.

It is easy to check whether a group is abelian from either its Cayley diagram or Cayley table.



## Direct products

An easy way to construct finite abelian groups is by taking **direct products** of cyclic groups.

This is an operation that can be done on any collection of groups.

For two groups,  $A$  and  $B$ , the Cartesian product is the set

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

### 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**.

The binary operations on  $A$  and  $B$  could be different. For example, in  $\mathbf{Tri} \times \mathbb{Z}_4$ :

$$(rf, 3) * (r^3, 1) = (rfr^3, 1 + 3) = (r^2f, 0).$$

These do *not* commute because

$$(r^3, 1) * (rf, 3) = (r^3rf, 3 + 1) = (f, 0).$$

## Direct products of cyclic groups

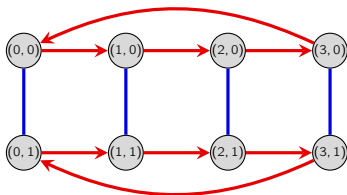
The **direct product** of  $\mathbb{Z}_n$  and  $\mathbb{Z}_m$  consists of the set of ordered pairs,

$$\mathbb{Z}_n \times \mathbb{Z}_m = \{(a, b) \mid a \in \mathbb{Z}_n, b \in \mathbb{Z}_m\}.$$

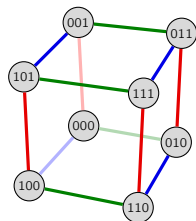
The binary operation is modulo  $n$  in the first component, and modulo  $m$  in the second component. In other words,

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2 \pmod{n}, b_1 + b_2 \pmod{m}).$$

Here are two examples:



$\mathbb{Z}_4 \times \mathbb{Z}_2$

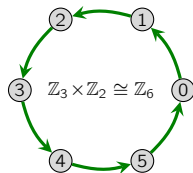
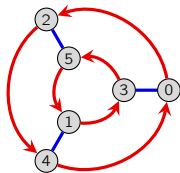
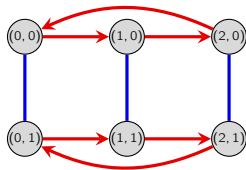


$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbf{Light}_3$

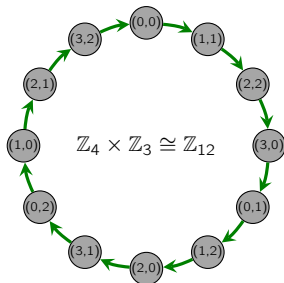
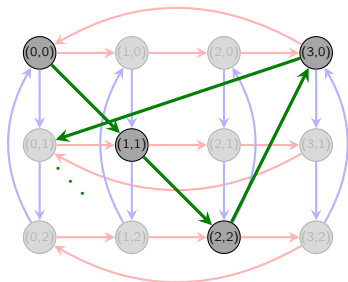
Though  $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ , we will usually write  $V_4 \cong C_2 \times C_2$  since we write  $V_4$  multiplicatively.

## Direct products of cyclic groups

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



Here is another example:



# Direct products of cyclic groups

## Proposition

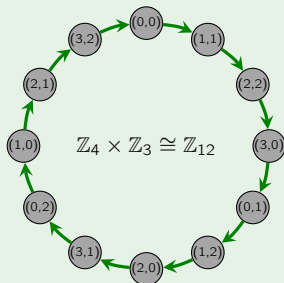
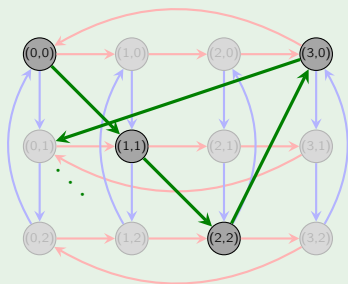
$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$  if and only if  $\gcd(n, m) = 1$ .

## Proof

“ $\Leftarrow$ ”: Suppose  $\gcd(n, m) = 1$ . We claim that  $(1, 1) \in \mathbb{Z}_n \times \mathbb{Z}_m$  has order  $nm$ .

$|k(1, 1)|$  is the smallest  $k$  such that “ $(k, k) = (0, 0)$ .” This happens iff  $n \mid k$  and  $m \mid k$ .

Thus,  $k = \text{lcm}(n, m) = nm$ . ✓



# 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 (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  $nm$ .

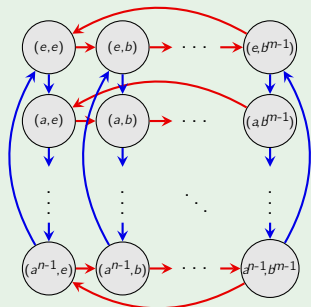
For convenience, we'll switch to "multiplicative notation", and denote our cyclic groups by  $C_n$ .

Clearly,  $\langle a \rangle = C_n$  and  $\langle b \rangle = C_m$ . Let's look at a Cayley diagram 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  $\text{lcm}(n, m) = nm$ . Therefore,  $\gcd(n, m) = 1$ . □





# The fundamental theorem of finite abelian groups

Though we do not yet have the tools needed to prove this result, it is worth knowing now.

## Classification theorem (by “prime powers”)

Every **finite abelian group**  $A$  is isomorphic to a **direct product of cyclic groups**, i.e., for some integers  $n_1, n_2, \dots, n_m$ ,

$$A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m},$$

where each  $n_i$  is a **prime power**, i.e.,  $n_i = p_i^{d_i}$ , where  $p_i$  is prime and  $d_i \in \mathbb{N}$ .

## Example

Up to isomorphism, there are 6 abelian groups of order  $200 = 2^3 \cdot 5^2$ :

$$\mathbb{Z}_8 \times \mathbb{Z}_{25}$$

$$\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

Finite abelian groups can alternatively be classified by their “**elementary divisors**.”

The mysterious terminology comes from the theory of modules (a graduate-level topic).

# The fundamental theorem of finite abelian groups

## Classification theorem (by “elementary divisors”)

Every **finite abelian group**  $A$  is isomorphic to a **direct product of cyclic groups**, i.e., for some integers  $k_1, k_2, \dots, k_m$ ,

$$A \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_m}.$$

where each  $k_i$  is a **multiple** of  $k_{i+1}$ .

## Example

Up to isomorphism, there are 6 abelian groups of order  $200 = 2^3 \cdot 5^2$ :

by “prime-powers”

$$\mathbb{Z}_8 \times \mathbb{Z}_{25}$$

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$$

$$\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

by “elementary divisors”

$$\mathbb{Z}_{200}$$

$$\mathbb{Z}_{100} \times \mathbb{Z}_2$$

$$\mathbb{Z}_{50} \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\mathbb{Z}_{40} \times \mathbb{Z}_5$$

$$\mathbb{Z}_{20} \times \mathbb{Z}_{10}$$

$$\mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$$

# 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:

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

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  $\mathbb{C}^+$ .

## Other abelian groups

It is clear that  $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ . However, there are many more subgroups of  $\mathbb{C}$  than these.

Most of the following are actually **rings**: additive groups also **closed under multiplication**. We'll study these more later.

### Definition

The **Gaussian integers** are the complex numbers of the form

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

We'll see  $\mathbb{Z}[\sqrt{-m}]$  and others when we encounter **rings of algebraic integers**.

The set of **polynomials** in  $x$  "*over the integers*" is a group under addition, denoted

$$\mathbb{Z}[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{Z}\}.$$

We can also look at certain subgroups, like the polynomials of degree  $\leq n$ .

Polynomials can be defined in multiple variables, like

$$\mathbb{Z}[x, y] = \left\{ \sum a_{ij} x^i y^j \mid a_{ij} \in \mathbb{Z}, \text{ all but finitely many } a_{ij} = 0 \right\},$$

or over a finite ring such as  $\mathbb{Z}_n$ .

# Dihedral groups

## Definition

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

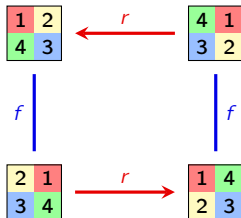
One possible choice of generators is

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

Using these generators, one (of many) ways to write the elements of  $D_n = \langle r, f \rangle$  is

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

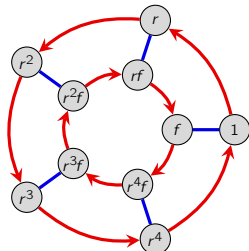
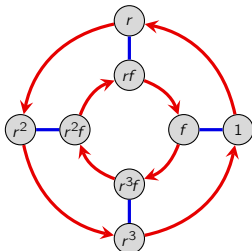
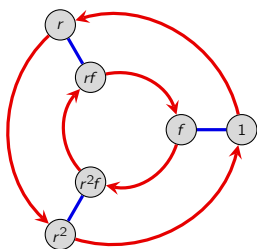
It is easy to check that  $rf = fr^{-1}$ :



## 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 canonical way to generate  $D_n$  is with two reflections:

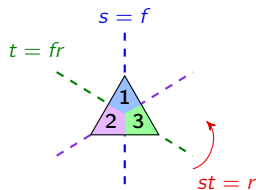
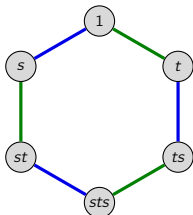
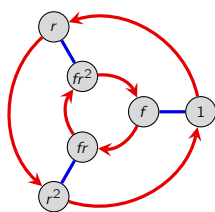
- $s := f$
- $t := fr = r^{n-1}f$

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

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

A group presentation with these generators is

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

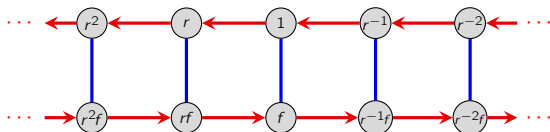


# Dihedral groups

## Definition

The **infinite dihedral group**, denoted  $D_\infty$ , has presentation

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



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

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





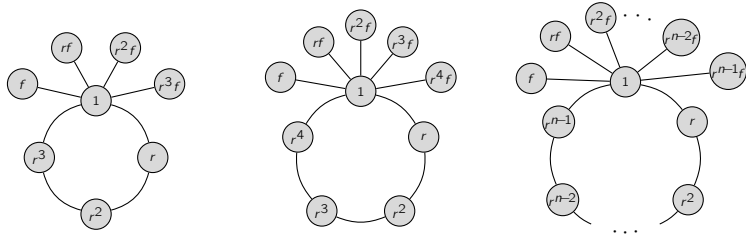
## Orbits in dihedral groups

The 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  $k = 0, 1, \dots, n-1$ .

Unless  $n$  is prime, the size- $n$  orbit will have smaller subsets that are orbits.

For example,  $\{1, r^2, r^4, \dots, r^{n-2}\}$  and  $\{1, r^{n/2}\}$  are orbits if  $n$  is even.



## 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      |

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

“Shrinking” a group in this way is called a **quotient**.

It yields a group of order 2 with the following Cayley table:

|     |     |     |
|-----|-----|-----|
|     | 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

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

The canonical **real representation of  $D_n$**  with  $2 \times 2$  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  $2 \times 2$  matrices is

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

*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!*

# Permutation groups

Loosely speaking, a **permutation** is an action that rearranges a set of objects.

## Definition

Let  $X$  be a set. A **permutation** of  $X$  is a bijection  $\pi: X \rightarrow X$ .

## Definition

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

If  $|X| = |Y|$ , then  $S_X \cong S_Y$ , and so we will usually work with  $S_n$ , which has order  $n! = n(n-1) \cdots 2 \cdot 1$ .

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

This is best seen with an example:

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

*"one-line notation"*



*"permutation diagram"*

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

*"cycle notation"*

## Permutation notations

**One-line notation:**  $\pi = 231654$ ,  $\sigma = 564123$

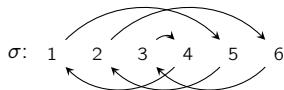
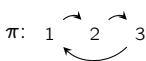
**Pros:**

- concise
- nice visualization of rearrangement

**Cons:**

- bad for combining permutations
- not clear where elements get mapped
- hard to compute the inverse

**Permutation diagram:**



**Pros:**

- can see where elements get mapped
- easy to compute inverses
- convenient for combining permutations

**Cons:**

- cumbersome to write
- can get tangled

**Cycle notation:**  $\pi = (123)(46)$ ,  $\sigma = (152634)$ ;

**Pros:**

- short and concise
- easy to see the disjoint cycles
- convenient for combining permutations

**Cons:**

- representation isn't unique
- not clear what  $n$  is

## Cycle notation

The cycle  $(1\ 4\ 6\ 5)$  means

*"1 goes to 4, which goes to 6, which does to 5, which goes back to 1."*

Thus, we can write  $(1\ 4\ 6\ 5) = (4\ 6\ 5\ 1) = (6\ 5\ 1\ 4) = (5\ 1\ 4\ 6)$ .

To find the **inverse** of a cycle, write it backwards:

$$(1\ 4\ 6\ 5)^{-1} = (5\ 6\ 4\ 1) = (1\ 5\ 6\ 4) = \dots$$

Though it's not necessary, we usually prefer to begin a cycle with its smallest number.

### Remark

Every permutation in  $S_n$  can be written in cycle notation as a product of **disjoint cycles**, and this is unique up to commuting and cyclically shifting cycles.

For example, consider the following permutation in  $S_{10}$ :



This is a product of four disjoint cycles. Since they are disjoint, they commute:

$$(1465)(23)(8\ 10\ 9) = (23)(8\ 10\ 9)(1465) = (23)(8\ 10\ 9)(1465) = \dots$$

## Composing permutations

### Remark

The **order** of a permutation is the least common multiple of the sizes of its disjoint cycles.

For example,  $(1\ 3\ 8\ 6)(2\ 9\ 7\ 4\ 10\ 5) \in S_{10}$  has order 12; this should be intuitive.

When cycles are not disjoint, order matters.

Many books compose permutations from right-to-left, due to function composition.

Since we have been using **right Cayley diagrams**, we will compose them from left-to-right.

### Notational convention

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

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

The main drawback about our convention is that it does not work well with function notation applied to elements, like  $\pi(i)$ .

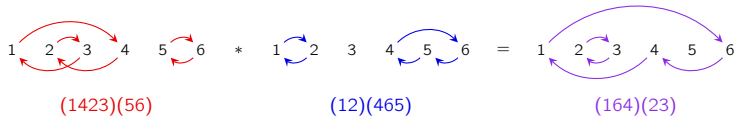
For example, notice that

$$(\pi\sigma)(i) = \sigma(\pi(i)) \neq \pi(\sigma(i)).$$

However, we will hardly ever use this notation, so that drawback is minimal.

## 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).

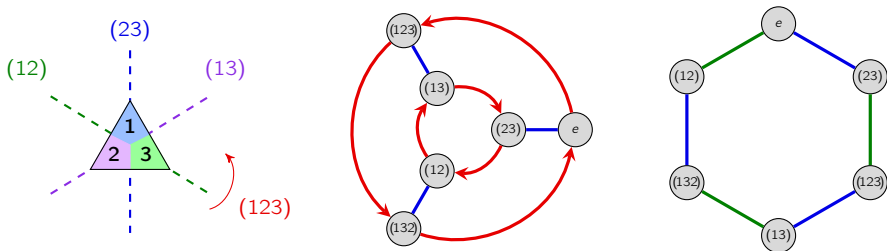


# The symmetric group

If we number the corners of an  $n$ -gon, every symmetry canonically defines a permutation.

However, not every permutation of the corners necessarily is a symmetry, unless  $n = 3$ .

Indeed, every permutation of  $\{1, 2, 3\}$  can be realized as an element of  $D_3$ .



## Remark

The groups  $D_n$  and  $S_n$  are isomorphic for  $n = 3$ , and non-isomorphic if  $n > 3$ .

## The symmetric group

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

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

Clearly,  $S_3$  canonically rearranges these configurations.

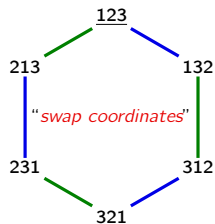
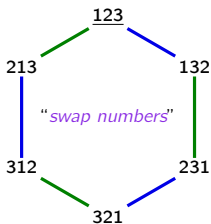
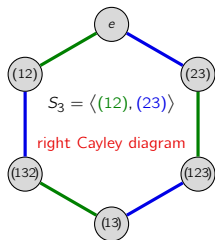
However, *there are two perfectly acceptable interpretations for "canonical."*

For example,  $(12)$  can be interpreted to mean

*"swap the numbers in the 1<sup>st</sup> and 2<sup>nd</sup> coordinates."*

Alternatively,  $(12)$  could mean

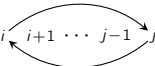
*"swap the numbers 1 and 2, regardless of where they are."*



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

# Transpositions

A **transposition** is a permutation that swaps two objects and fixes the rest, e.g.:

$$\tau = (ij): \quad 1 \quad 2 \quad \cdots \quad i-1 \quad i \quad i+1 \quad \cdots \quad j-1 \quad j \quad j+1 \quad \cdots \quad n-1 \quad n$$


An **adjacent transposition** is one of the form  $(i \ i+1)$ .

The following result should be intuitive, if one thinks about rearranging  $n$  objects in a row.

## Remark

There are two canonical types of generating sets for  $S_n$ :

- **Adjacent transpositions:**

$$S_n = \langle (1 \ 2), (2 \ 3), \dots, (n-1 \ n) \rangle.$$

- **Any transposition** and **any  $n$ -cycle**, e.g.,

$$S_n = \langle (1 \ 2), (1 \ 2 \ \cdots \ n-1 \ n) \rangle.$$

## Polytopes and platonic solids

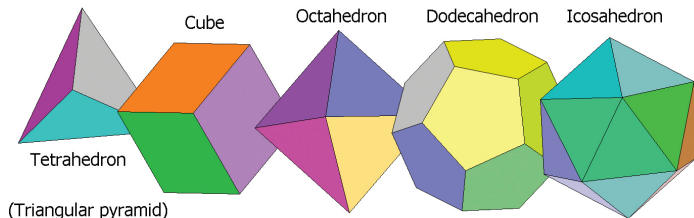
A **polytope** is a finite region of  $\mathbb{R}^n$  enclosed by finitely many hyperplanes.

2D polytopes are *polygons*, and 3D polytopes are **polyhedra**.

The formal definition of a **regular polytope** involves a technical condition of its symmetry group.

Informally, it means all faces and all vertices are identical and indistinguishable – higher-dimensional analogues of regular polygons.

There are exactly five regular polyhedra, called **Platonic solids**.



## Archimedean solids

More general than the Platonic solids are the **Archimedean solids**.

These are non-regular **convex uniform polyhedra** built from regular polygons.

Though they can involve different polygons, all vertices are locally identical.

In the third century B.C.E., Archimedes classified all 13 such polyhedra.

Five are “truncated versions” of the Platonic solids – formed by chopping off vertices.

The others consist of

- the chiral “**snub cube**” and “**snub dodecahedron**”
- “hybrids” such as the **icosidodecahedron**
- truncated versions of these hybrids.

The Cayley diagram of  $S_4$  can be arranged on the skeletons of several of these.

## Archimedean solids



cuboctahedron



icosidodecahedron



truncated  
tetrahedron



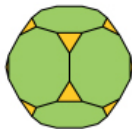
truncated  
octahedron



truncated cube



truncated  
icosahedron



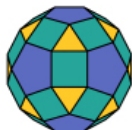
truncated  
dodecahedron



small  
rhombicuboctahedron



great  
rhombicuboctahedron



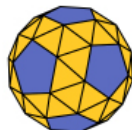
small  
rhombicosidodecahedron



great  
rhombicosidodecahedron



snub cube



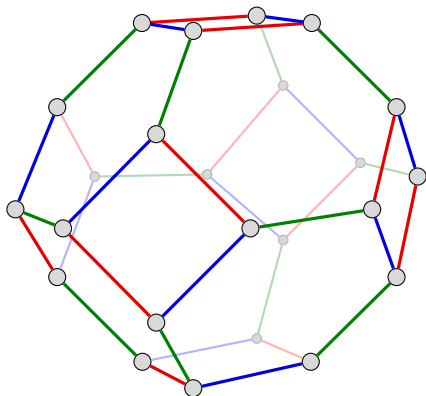
snub dodecahedron

© Encyclopædia Britannica, Inc.

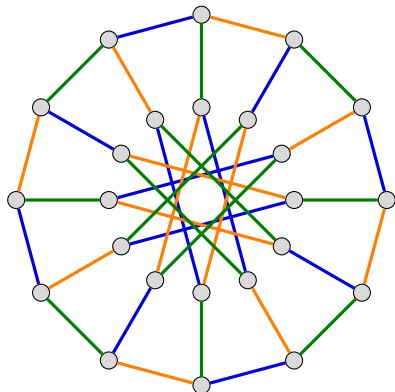
## Archimedean solids and $S_4$

Below are Cayley diagrams for the group

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



truncated octahedron; "*permutahedron*"



"*Nauru graph*"

**Exercise:** On the permutahedron, construct the Cayley diagram for

$$S_4 = \langle (12), (1234) \rangle.$$

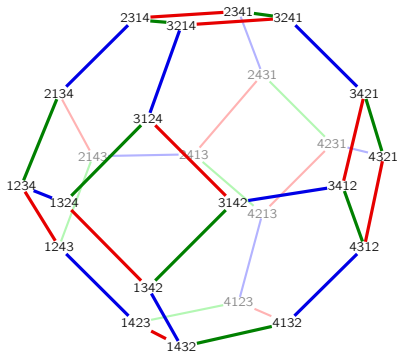
# The left and right permutahedra

## Definition

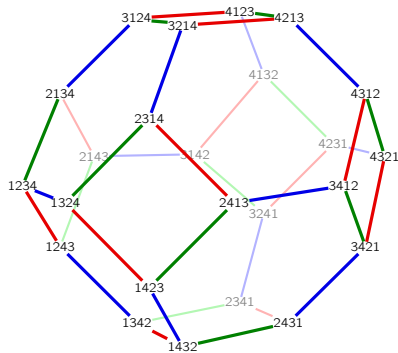
The (right)  $n$ -permutahedron is the convex hull of the  $n!$  permutations of  $(1, \dots, n) \in \mathbb{R}^n$ .

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

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



"swap coordinates"

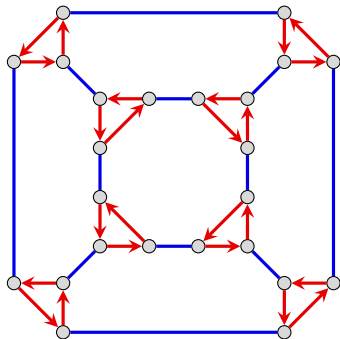


"swap numbers"

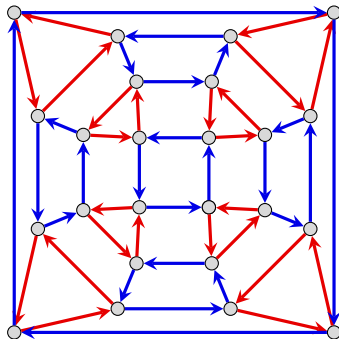


## Other Archimedean solids and $S_4$

Here are two more Cayley diagrams for  $S_4$ .



*truncated cube*



*rhombicuboctahedron*

We will leave it as an exercise to determine the generators.

## Even and odd permutations

### Remark

Even though every permutation in  $S_n$  can be written as a product of transpositions, there may be many ways to do this.

For example:  $(1\ 3\ 2) = (1\ 2)(2\ 3) = (1\ 2)(2\ 3)(2\ 3)(2\ 3) = (1\ 2)(2\ 3)(1\ 2)(1\ 2)$ .

### Proposition

The **parity** of the number of transpositions of a fixed permutation is unique.

### Definition

An **even permutation** in  $S_n$  can be written with an even number of transpositions. An **odd permutation** requires an odd number.

### Remark

The product of:

- two **even** permutations is **even**
- two **odd** permutations is **even**
- an **even** and an **odd** permutation is **odd**.

# The alternating groups

## Definition

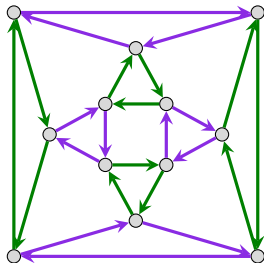
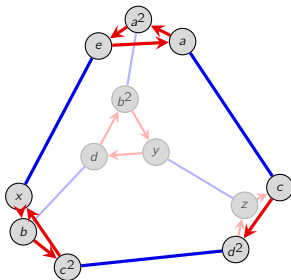
The set of even permutations in  $S_n$  is the **alternating group**, denoted  $A_n$ .

## Proposition

Exactly half of the permutations in  $S_n$  are even, and so  $|A_n| = \frac{n!}{2}$ .

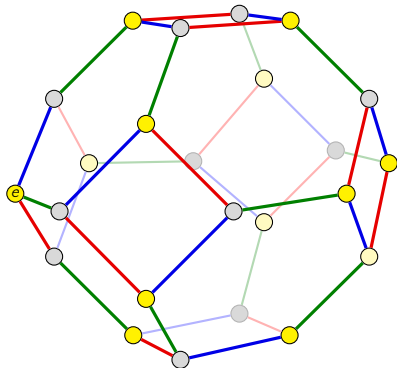
Rather than prove this using (messy) elementary methods now, we'll wait until we see the **isomorphism theorems** to get a 1-line proof.

Here are Cayley diagrams for  $A_4$  on a **truncated tetrahedron** and **cubeoctahedron**.

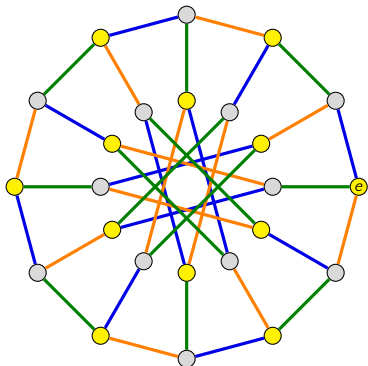


## The appearance of $A_4$ in Cayley diagrams for $S_4$

Let's highlight in yellow the even permutations in Cayley diagrams 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**.

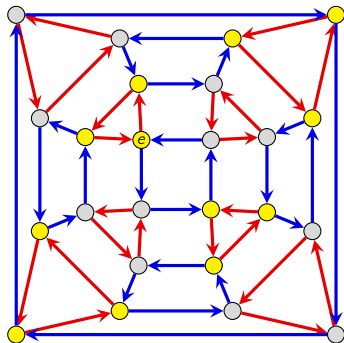
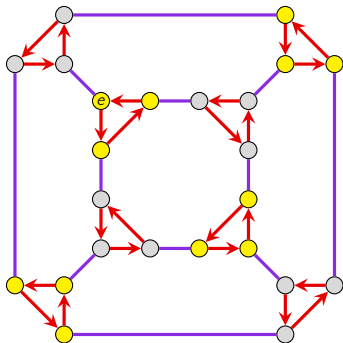
## The appearance of $A_4$ in Cayley diagrams for $S_4$

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 diagrams, blue arrows flip the sign of the permutation; red arrows do not.

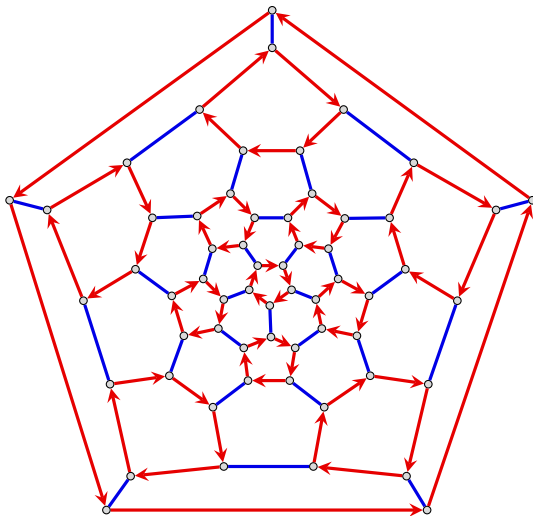
Once again, even permutations are highlighted in yellow.



## A very important group

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

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

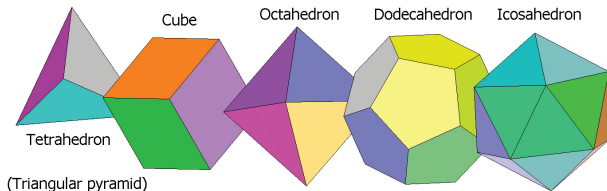


## Symmetry groups of Platonic solids

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”).

## Cayley's theorem

A set of permutations that forms a group is called a **permutation group**.

A fundamental theorem by British mathematician Arthur Cayley (1821–1895) says that every finite group can be thought of as a collection of permutations.

This is clear for groups of symmetries like  $V_4$ ,  $C_n$ , or  $D_n$ , but less so for groups like  $Q_8$ .

### Cayley's theorem

Every finite group is isomorphic to a collection of permutations, i.e., some subgroup of  $S_n$ .

We don't have the mathematical tools to prove this, but we'll get a 1-line proof when we study group actions.

A natural first question to ask is the following:

*Given a group, how do we associate it with a set of permutations?*

We'll see two algorithms which give strong intuition for why Cayley's theorem is true.



## Constructing permutations from a Cayley diagram

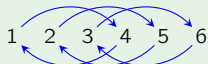
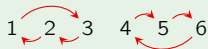
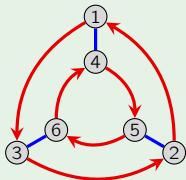
Here is an algorithm given a **Cayley diagram** with  $n$  nodes:

1. number the nodes 1 through  $n$ ,
2. interpret each arrow type in the Cayley diagram as a permutation.

Take the permutations corresponding to the generators.

### Example

Let's try this with  $D_3 = \langle r, f \rangle$ .



We see that  $D_3$  is isomorphic to the subgroup  $\langle (132)(456), (14)(25)(36) \rangle$  of  $S_6$ .

## Constructing permutations from a Cayley table

Here is an algorithm given a [Cayley table](#) with  $n$  elements:

1. replace the table headings with 1 through  $n$ ,
2. make the appropriate replacements throughout the rest of the table,
3. interpret each column as a permutation.


Take the permutations corresponding to *any* generating set.

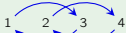
### Example


Let's try this with the multiplication table for  $V_4 = \langle v, h \rangle$ .

|   | 1 | 2 | 3 | 4 |   |
|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |   |
| 2 | 2 | 1 | 4 | 3 |   |
| 3 | 3 | 3 | 4 | 1 | 2 |
| 4 | 4 | 4 | 3 | 2 | 1 |

Column 1: 1 2 3 4

Column 2: 

Column 3: 

Column 4: 

We see that  $V_4$  is isomorphic to the subgroup  $\langle (12)(34), (13)(24) \rangle$  of  $S_4$ .

## Permutation matrices

We have seen how to represent groups of symmetries such as  $V_4$ ,  $C_n$ , and  $D_n$  as matrices.

Permuting coordinates of  $\mathbb{R}^n$  is also a linear transformation.

Every permutation can be represented by an  $n \times n$  **permutation matrix**,  $P_\pi$ .

For an example of this, consider the following permutation  $\pi \in S_5$ :

$$\begin{array}{c|ccccc} i & 1 & 2 & 3 & 4 & 5 \\ \hline \pi(i) & 3 & 1 & 2 & 5 & 4 \end{array} \quad \begin{array}{c} \curvearrowright \\ 1 \quad 2 \quad 3 \\ \curvearrowleft \end{array} \quad \begin{array}{c} \curvearrowright \\ 4 \quad 5 \\ \curvearrowleft \end{array} \quad \pi = (132)(45)$$

The matrix  $P_\pi$  permutes the entries of a column vector:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \\ x_5 \\ x_4 \end{bmatrix},$$

It permutes the entries of a row vector (by coordinates):

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} x_3 & x_1 & x_2 & x_5 & x_4 \end{bmatrix}.$$

# Permutation matrices

## Definition

Given an element  $\pi \in S_n$ , the corresponding **permutation matrix** is the  $n \times n$  matrix

$$P_\pi = (p_{ij}), \quad p_{ij} = \begin{cases} 1 & \pi(i) = j \\ 0 & \text{otherwise.} \end{cases}$$

Here are several more examples of permutation matrices.

$$P_{(12)(34)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad P_{(134)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad P_{(1234)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Notice that the difference between left and right multiplication is:

$P_\pi P_\sigma x$       **Right-to-left:** "Start with  $x$ , apply  $\sigma$ , then  $\pi$ "

$x^T P_\pi P_\sigma$       **Left-to-right:** "Start with  $x^T$ , apply  $\pi$ , then  $\sigma$ "

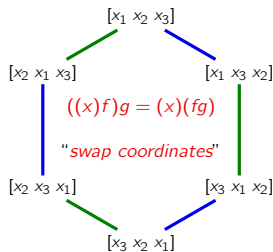
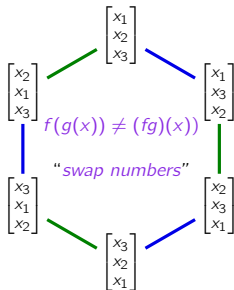
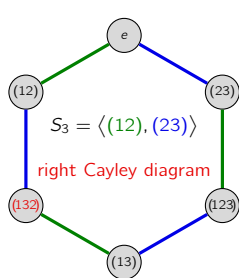
It does not matter whether we use row or column vectors, but we must be careful.

- **Column vectors** correspond to multiplying **right-to-left**, as in **function composition**.
- **Row vectors** correspond to multiplying **left-to-right**, which has been **our standard**.

Our left-to-right multiplication convention is more compatible with row vectors

$$P_{(12)}P_{(23)}\mathbf{v} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_3 \\ x_1 \\ x_2 \end{bmatrix} = P_{(132)}\mathbf{v}.$$

$$\mathbf{v}^T P_{(12)}P_{(23)} = [x_1 \quad x_2 \quad x_3] \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = [x_1 \quad x_2 \quad x_3] \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \\ = [x_2 \quad x_3 \quad x_1] = \mathbf{v}^T P_{(132)}.$$



## Generalizing the quaternion group

The quaternions are an abstract way to generalize the complex number  $i = \sqrt{-1}$ :

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

### Exploratory question

Why does this work? What if we define  $\ell = \sqrt{-1}$ ? Would such a construction even work, and if so, how?

One way to answer this is to represent  $Q_8$  with matrices.

Since  $i = \sqrt{-1} = e^{2\pi i/4}$  is a fourth root of unity, it generates a cyclic group

$$C_4 \cong \{1, i, -1, -i\} \cong \left\langle \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \right\}.$$

If we define the matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad R = R_4 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad T = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix},$$

then it is easy to check that  $R^2 = S^2 = T^2 = RST = -I$ .

Thus, we have a representation of the quaternion group:

$$Q_8 \cong \langle R, S \mid R^2 = S^2 = T^2 = RST = -I \rangle.$$

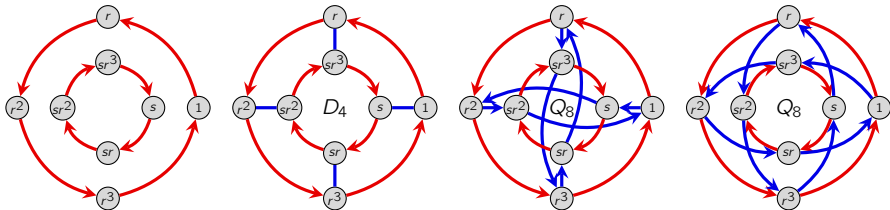
# Generalizing the quaternion group

## Exercise

If every element of  $G$  is its own inverse (i.e.,  $g^2 = e$  for all  $g \in G$ ) then it must be abelian.

This means that any nonabelian group  $G$  of order 8 must have an element  $r$  of order 4.

That is, we must have a “partial Cayley diagram” like the following (left):

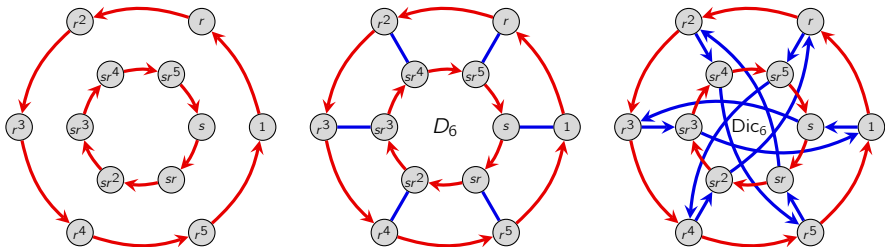


It's not hard to check that these are the only two ways to complete such a nonabelian diagram, up to isomorphism.

We can generalize both of these constructions from  $2 \cdot 4 = 8$  nodes to  $2m$  nodes.

## The dicyclic groups

Let's look at this construction for  $n = 6$ , so  $|G| = 12$ . Let  $G = \langle r, s \rangle$  with  $|r| = 6$ .



The first group is **dihedral**, and has presentation

$$D_6 = \langle r, s \mid r^6 = 1, s^2 = 1, srs = r^{-1} \rangle.$$

The second group is called **dicyclic**, and has presentation

$$\text{Dic}_6 = \langle r, s \mid r^6 = 1, s^4 = 1, r^3 = s^2, rsr = s \rangle.$$

Note that  $\text{Dic}_4 \cong Q_8$ , under the correspondence  $r = i$  and  $s = j$ .

### Key idea

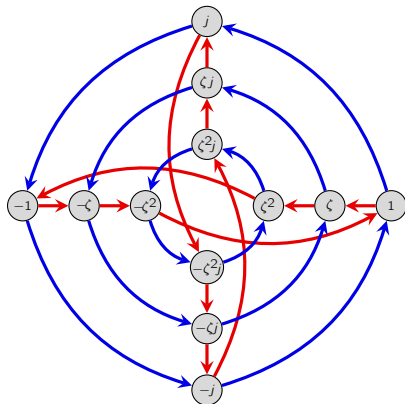
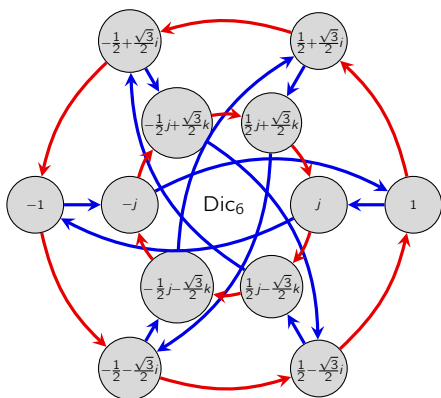
Think of  $r$  as a  $60^\circ$  rotation. That is,  $r = \zeta_6 = e^{2\pi i/6} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$  is a “cube root of  $-1$ .”



## The dicyclic groups

In other words, we can construct  $\text{Dic}_6 = \langle r, s \rangle = \langle \zeta_6, j \rangle$  as follows:

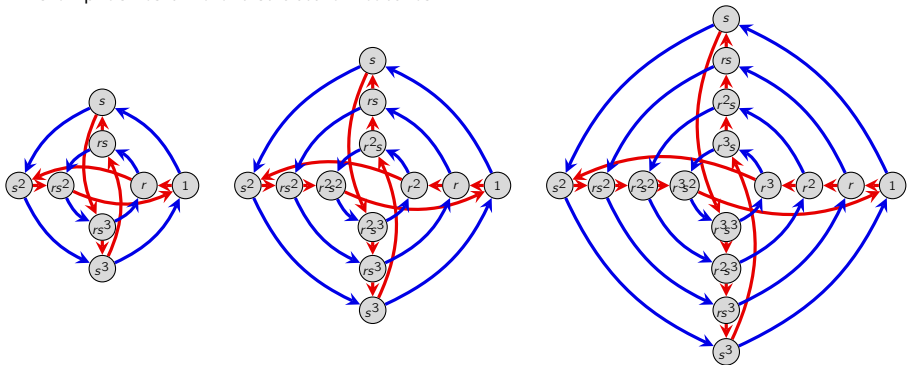
- start with the quaternion group  $Q_8 = \langle i, j \rangle = \langle \zeta_4, j \rangle$
- replace  $i = e^{2\pi i/4} = \zeta_4$  with the 6<sup>th</sup> root of unity  $\zeta_6 = e^{2\pi i/6} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$
- multiplication rules  $ij = k$  and  $ji = -k$  remain unchanged.



## The dicyclic groups

Here's another layout of the Cayley diagram of  $\text{Dic}_n = \langle r, s \rangle = \langle \zeta_n, j \rangle$ , for  $n = 4, 6, 8$ .

This emphasizes different structural features.

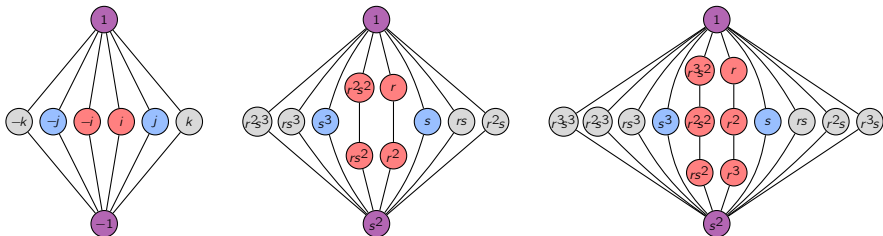


In the next chapter, we'll explore the subgroups of the dicyclic groups, which highlight even more different structural features.

We'll see why when  $n = 2^m$ ,  $\text{Dic}_n$  is also called the **generalized quaternion group**,  $Q_{2^m}$ .

## The dicyclic groups

Let's construct the cycle graphs of  $\text{Dic}_n = \langle r, s \rangle = \langle \zeta_n, j \rangle$ , for  $n = 4, 6, 8$ :



The cycle graphs highlight properties that can be hidden in the Cayley diagram:

- there is a unique element  $s^2 = r^n$  of order 2 (we can call this  $-1$ )
- there are either  $n$  or  $n + 2$  elements of order 4, depending on the parity of  $n$ .

Let's compare the dihedral and dicyclic groups:

- $D_n$ : One size- $n$  orbit  $\langle r \rangle$ , and  $n$  size-2 orbits, all intersecting in  $\langle 1 \rangle$ .
- $\text{Dic}_n$ : One size- $n$  orbit  $\langle r \rangle$ , and  $n/2$  size-4 orbits, all intersecting in  $\langle s^2 \rangle = \{\pm 1\}$ .

## A representation of the dicyclic group

Recall that we can represent  $D_n$  with  $2 \times 2$  matrices as

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

We can also represent the quaternion group as

$$Q_8 = \{ \pm 1, \pm i, \pm j, \pm k \} \cong \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \right\}.$$

### Remark

The dicyclic group  $\text{Dic}_n = \langle r, s \rangle = \langle \zeta_n, j \rangle$  can be thought of as being generated by:

- a primitive  $n^{\text{th}}$  root of unity, i.e., a rotation of  $2\pi/n$  radians,
- the “imaginary number”  $j \in Q_8$ .

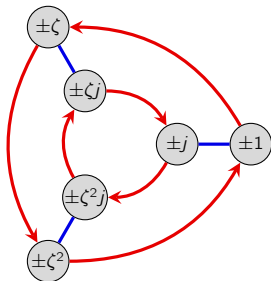
We now have a canonical representation with  $2 \times 2$  matrices:

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

## 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.



|                 |                 |                 |                 |                 |                 |                 |
|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
|                 | $\pm 1$         | $\pm \zeta$     | $\pm \zeta^2$   | $\pm j$         | $\pm \zeta j$   | $\pm \zeta^2 j$ |
| $\pm 1$         | $\pm 1$         | $\pm \zeta$     | $\pm \zeta^2$   | $\pm j$         | $\pm \zeta j$   | $\pm \zeta^2 j$ |
| $\pm \zeta$     | $\pm \zeta$     | $\pm \zeta^2$   | $\pm 1$         | $\pm \zeta j$   | $\pm \zeta^2 j$ | $\pm j$         |
| $\pm \zeta^2$   | $\pm \zeta^2$   | $\pm 1$         | $\pm \zeta$     | $\pm \zeta^2 j$ | $\pm j$         | $\pm \zeta j$   |
| $\pm j$         | $\pm j$         | $\pm \zeta^2 j$ | $\pm \zeta j$   | $\pm 1$         | $\pm \zeta^2$   | $\pm \zeta$     |
| $\pm \zeta j$   | $\pm \zeta j$   | $\pm j$         | $\pm \zeta^2 j$ | $\pm \zeta$     | $\pm 1$         | $\pm \zeta^2$   |
| $\pm \zeta^2 j$ | $\pm \zeta^2 j$ | $\pm \zeta j$   | $\pm j$         | $\pm \zeta^2$   | $\pm \zeta$     | $\pm 1$         |

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

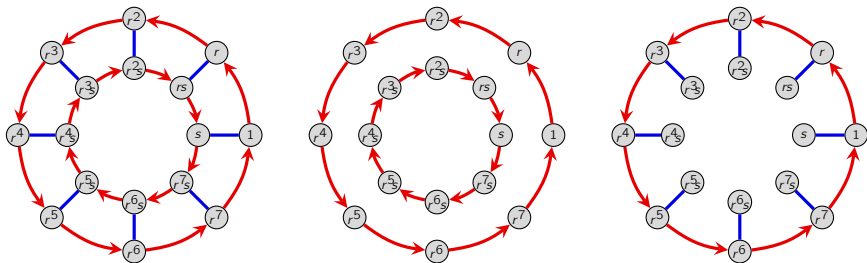
*"the product of any element in  $\{\zeta j, -\zeta j\}$  with any element in  $\{\zeta^2 j, -\zeta^2 j\}$  is in  $\{\zeta^2, -\zeta^2\}$ ."*

## Generalizing the dihedral groups

In our construction of the dicyclic groups, we started with a Cayley diagram of  $D_n = \langle r, f \rangle$ .

We then removed the blue arcs and investigated how we could re-wire them.

But 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

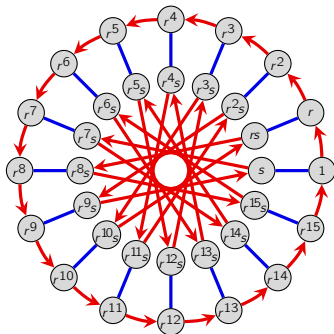
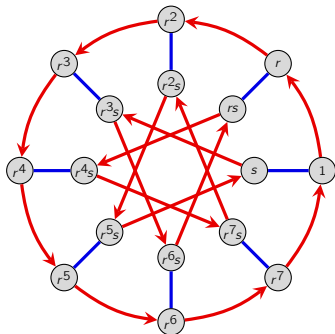
- has an element  $r$  of order  $n$
- has an element  $s \notin \langle r \rangle$  of order 2.

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

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

## Semidihedral groups

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



### Definition

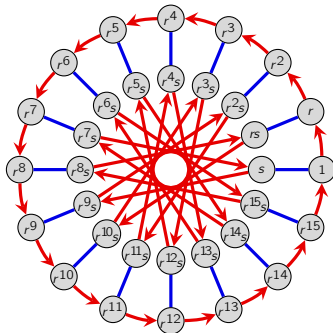
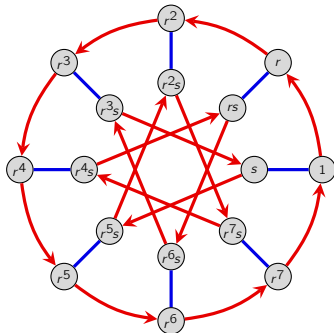
For each power of two, the **semidihedral group** of order  $2^n$  is defined by

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

*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

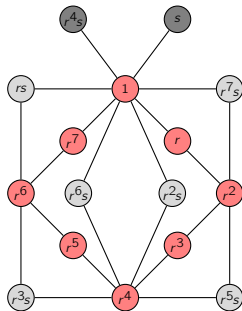
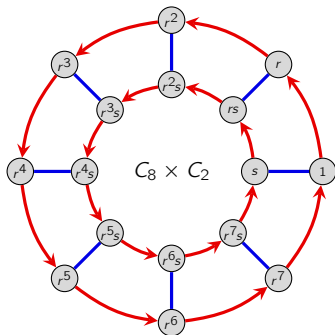
$$\text{SA}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1, srs = r^{2^{n-2}+1} \rangle.$$



## One more re-wiring

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

Here is its Cayley diagram and cycle graph.



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

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

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

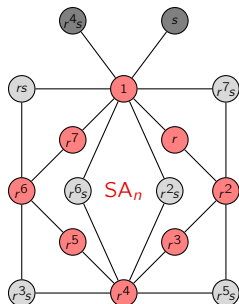
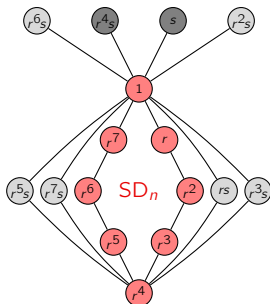
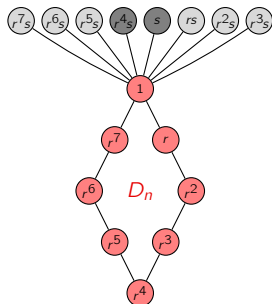
$$srs = r^{-1} \text{ (dihedral),} \quad srs = r^{2^{n-2}-1} \text{ (semidihedral),} \quad srs = r^{2^{n-2}+1} \text{ (semiabelian).}$$

## Dihedral vs. semidihedral 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 diagrams 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. semidihedral vs. semiabelian groups

Recall our canonical representations of the cyclic and dihedral groups

$$C_n \cong \left\langle \left[ \begin{array}{cc} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{array} \right] \right\rangle, \quad D_n \cong \left\langle \left[ \begin{array}{cc} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{array} \right], \left[ \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right] \right\rangle,$$

where  $\zeta_n = e^{2\pi i/n}$  is an  $n^{\text{th}}$  root of unity.

When  $n$  is even, we can define the **dicyclic groups** by the representation

$$\text{Dic}_n \cong \left\langle \left[ \begin{array}{cc} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{array} \right], \left[ \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right] \right\rangle.$$

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**:

$$\text{SD}_n \cong \left\langle \left[ \begin{array}{cc} \zeta_n & 0 \\ 0 & -\bar{\zeta}_n \end{array} \right], \left[ \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right] \right\rangle, \quad \text{SA}_n \cong \left\langle \left[ \begin{array}{cc} \zeta_n & 0 \\ 0 & -\zeta_n \end{array} \right], \left[ \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right] \right\rangle.$$

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 $2^n$

We'll understand the following better when we study semi-direct products of groups.

### Theorem

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

1. The **dihedral group**  $D_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1, srs = r^{-1} \rangle$ .
2. The **dicyclic group**  $\text{Dic}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^4 = 1, r^{2^{n-2}} = s^2, rsr = s \rangle$ .
3. The **semidihedral group**  $\text{SD}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1, srs = r^{2^{n-2}-1} \rangle$ .
4. The **semiabelian group**  $\text{SA}_{2^{n-1}} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1, srs = r^{2^{n-2}+1} \rangle$ .

As we did before, we can ask:

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

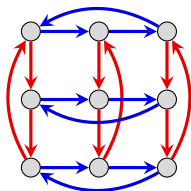
## Revisiting direct products

Let  $A, B$  be groups with identity elements  $1_A$  and  $1_B$ . Suppose we have a

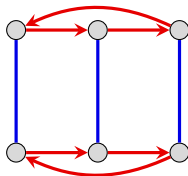
- Cayley diagram of  $A$  with generators  $a_1, \dots, a_k$ ,
- Cayley diagram of  $B$  with generators  $b_1, \dots, b_\ell$ .

We can create a Cayley diagram for  $A \times B$ , by taking

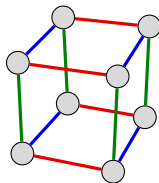
- Vertex set:  $\{(a, b) \mid a \in A, b \in B\}$ ,
- Generators:  $(a_1, 1_B), \dots, (a_k, 1_B)$  and  $(1_A, b_1), \dots, (1_A, b_\ell)$ .



$C_3 \times C_3$



$C_3 \times C_2$



$C_2 \times C_2 \times C_2$

### Remark

“ $A$ -arrows” are independent of “ $B$ -arrows.” Algebraically, this means

$$(a, 1_B) * (1_A, b) = (a, b) = (1_A, b) * (a, 1_B).$$

## Revisiting direct products

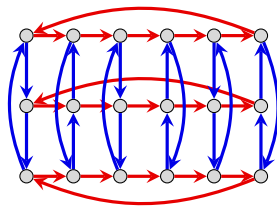
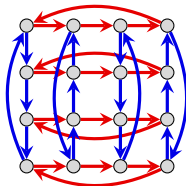
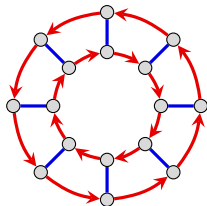
### Remark

Just because a group is not written with  $\times$  does not mean that there is not secretly a direct product structure lurking behind the scenes.

We have already seen that  $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ , and that  $C_6 \cong C_3 \times C_2$ .

However, sometimes it is even less obvious.

Two of the following three groups secretly have a direct product structure.



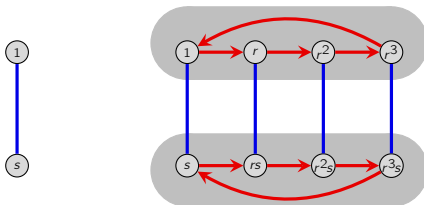
(And it's probably not the two you think.)

# Semidirect products

Semidirect products are a more general construction than the direct product.

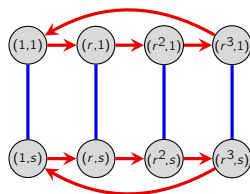
They can be thought of as a “twisted” version of the direct product.

To motivate this, consider the following “inflation method” for constructing the Cayley diagram of a direct product:



Start with a copy of  $B = C_2$

Inflate each node, insert  $A = C_4$  in each and connect corresponding nodes with edges



“pop” each inflated node to get the direct product  $C_4 \times C_2$

Consider this process, but with the red arrows reversed in the bottom inflated node.

This would result in a Cayley diagram for the group  $D_4$ .

We say that  $D_4$  is the **semidirect product** of  $C_4$  and  $C_2$ , written  $D_4 \cong C_4 \rtimes C_2$ .

## Semidirect products

Reversing the red arrows worked is because it was a **structure-preserving rewiring**.

Formally, this is an **automorphism**, which is an **isomorphism from a group to itself**.

We'll learn more about this when we study homomorphisms. Just know that it's a bijection

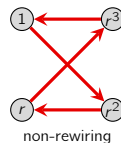
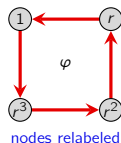
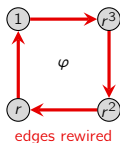
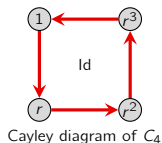
$$\varphi: G \longrightarrow G$$

satisfying some extra properties.

There are two ways to describe a rewiring:

- fix the position of the nodes and **rewire the edges**
- fix the position of the edge and **relabel the nodes**.

This is best seen with an example:



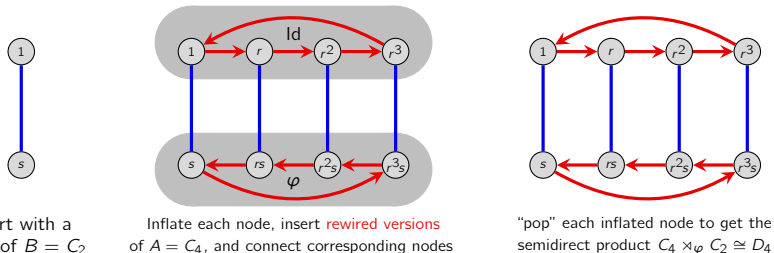
The diagram on the right isn't allowed because it doesn't preserve the algebraic structure.



## Semidirect products

Semidirect products can be constructed via the “inflation process” for  $A \times B$ , but *insert  $\varphi$ -rewired copies* of the Cayley diagram for  $A$  into inflated nodes of  $B$ .

Let’s construct  $A \rtimes B$  for  $A = C_4$  and  $B = C_2$ , with the rewiring  $\varphi$  from the previous slide.



In the middle diagram, each inflated node of  $B = C_2 = \langle s \rangle$  is labeled with a re-wiring.

Formally, this is a just map

$$\theta: C_2 \longrightarrow \text{Aut}(C_4), \quad \theta(g) = \begin{cases} \text{ld} & g = 1 \\ \varphi & g = s, \end{cases}$$

where  $\theta(g)$  specifies which re-wiring gets put into the inflated node  $g$  of  $C_2$ .

## Semidirect products

There are strong restrictions for inserting rewirings of the Cayley diagram of  $A$  into  $B$ .

The map  $\theta$  must be a structure-preserving map, called a **homomorphism**.

If we stick a  $\varphi$ -rewiring into the inflated node  $b \in B$ , then we must insert a  $\varphi^2$ -rewiring into node  $b^2 \in B$ , and so on.

### Definition (informal)

Consider groups  $A, B$ , and a structure-preserving map

$$\theta: B \longrightarrow \text{Aut}(A)$$

to the **set of rewirings of  $A$** . The **semidirect product**  $A \rtimes_{\theta} B$ , is constructed by:

- inflating the nodes of the Cayley diagram of  $B$ , [*mnemonic*:  $B$  for “balloon”]
- inserting a  $\theta(b)$ -rewiring of the **Cayley diagram  $A$**  into **node  $b$  of  $B$** ,
- For each **edge bewteen  $B$ -nodes**, connect corresponding pairs of  $A$ -nodes with that edge.

## Semidirect products

### Key point

For groups  $A, B$  and map

$$\theta: B \longrightarrow \text{Aut}(A),$$

the image  $\theta(b)$  can be thought of as "*which rewiring node  $b \in B$  gets label with*".

Any group  $A$  always has a trivial rewiring.

### Remark

For the trivial map  $\theta: B \longrightarrow \text{Aut}(A)$  sending everything to the identity rewiring

$$A \rtimes_{\theta} B = A \times B.$$

For any  $n$ , there is a rewiring  $\varphi$  of  $C_n = \langle r \rangle$  that "reverses all of the  $r$ -arrows".

The semidirect product of  $C_n$  and  $C_2 = \{1, s\}$ , with respect to

$$\theta: C_2 \longrightarrow \text{Aut}(C_n), \quad \theta(g) = \begin{cases} \text{Id} & g = 1 \\ \varphi & g = s, \end{cases}$$

is  $D_n \cong C_n \rtimes_{\theta} C_2$ .

# Semidirect products

## Reasons for introducing semidirect products this early

- it helps us understand a new way to construct groups
- it helps us understand the structure of some groups we've already seen
- thinking about *what* works in this process and *why*, helps us gain a more holistic understanding about group theory
- it will be easier to learn advanced concepts such as automorphisms if we get a preview of them in advance, and gain intuition

## Proposition

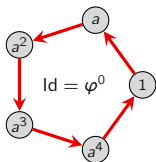
The set of rewirings of a Cayley diagram of  $G$  forms a group, denoted  $\text{Aut}(G)$ .

Moreover, this group does not depend on the Cayley diagram, but on the group itself.

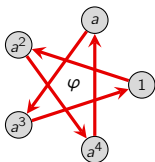
## Rewirings and the automorphism group

There are four rewirings (i.e., automorphisms) of the Cayley diagram of  $C_5 = \langle a \rangle$ .

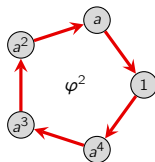
Every rewiring can be realized by iterating the "doubling map"  $\varphi: C_5 \rightarrow C_5$  that replaces each instance of  $a$  with  $a^2$ , i.e., a length- $k$  path with a length- $2k$  path.



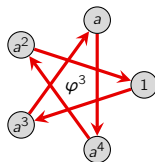
starting diagram



$a^1 \mapsto (a^1)^2 = a^2$



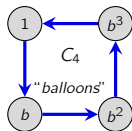
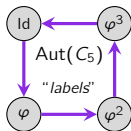
$a^2 \mapsto (a^2)^2 = a^4$



$a^4 \mapsto (a^4)^2 = a^3$

Notice that the rewirings form a group:

$$\text{Aut}(C_5) = \{1, \varphi, \varphi^2, \varphi^3\} \cong C_4$$



### Remark

For any group  $G$ , the set  $\text{Aut}(G)$  of rewirings forms a group, called its **automorphism group**.

## The automorphism group of $C_n$

Each automorphism is defined by where it sends a generator:  $r \mapsto r^k$ .

"each red arrow gets multiplied by  $k$ "

The group  $\text{Aut}(C_n)$  is isomorphic to the group with operation **multiplication modulo  $n$** :

$$U_n = \{k > 0 \mid \gcd(n, k) = 1\}.$$

**Example:**

$$\text{Aut}(C_7) \cong U_7 = \{1, 2, 3, 4, 5, 6\} = \langle 3 \rangle \cong C_6$$

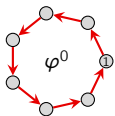
$$2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1$$

$$3^0 = 1, \quad 3^1 = 3, \quad 3^2 = 2$$

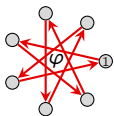
$$3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5$$

|   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|
|   | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

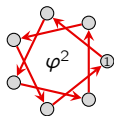
Since  $U_7 = \langle 3 \rangle$ , the re-wirings of  $C_7$  are generated by the "tripling map"  $r \xrightarrow{\varphi} r^3$ .



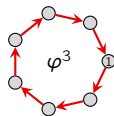
$$C_7 = \langle r \rangle$$



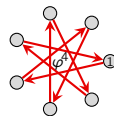
$$r^1 \mapsto (r^1)^3 = r^3$$



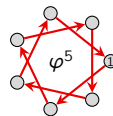
$$r^3 \mapsto (r^3)^3 = r^2$$



$$r^2 \mapsto (r^2)^3 = r^6$$



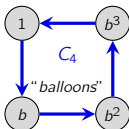
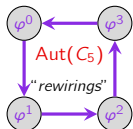
$$r^6 \mapsto (r^6)^3 = r^4$$



$$r^4 \mapsto (r^4)^3 = r^5$$

# An example: the 1<sup>st</sup> semidirect product of $C_5$ and $C_4$

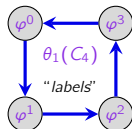
Let's construct a semidirect product  $C_5 \rtimes_{\theta_1} C_4$ :



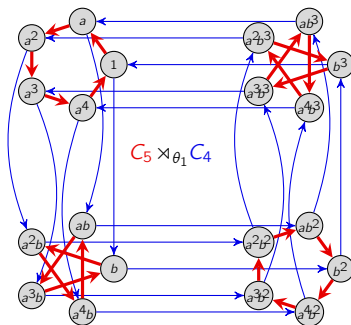
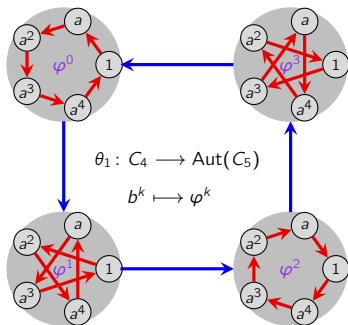
"labeling map"

$$C_4 \xrightarrow{\theta_1} \text{Aut}(C_5)$$

$$b^k \mapsto \varphi^k$$

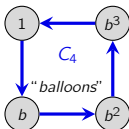
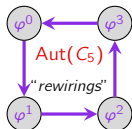


Stick in **rewired copies of A**, and then reconnect the **B-arrows**.



# An example: the 2<sup>nd</sup> semidirect product of $C_5$ and $C_4$

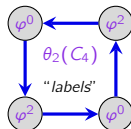
Let's now construct a different semidirect product,  $C_5 \rtimes_{\theta_2} C_4$ :



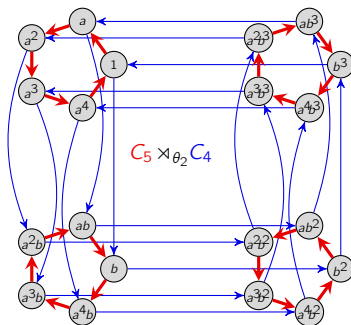
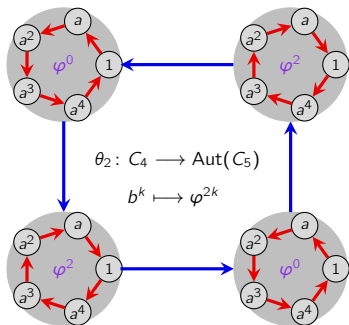
"labeling map"

$$C_4 \xrightarrow{\theta_2} \text{Aut}(C_5)$$

$$b^k \mapsto \varphi^{2^k}$$



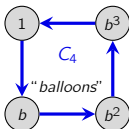
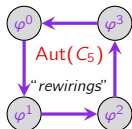
Stick in **rewired copies of A**, and then reconnect the **B-arrows**.





# An example: the 3<sup>rd</sup> semidirect product of $C_5$ and $C_4$

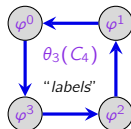
Let's construct another semidirect product  $C_5 \rtimes_{\theta_3} C_4$ :



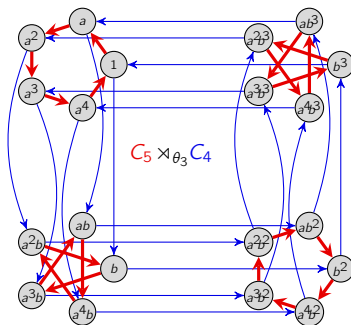
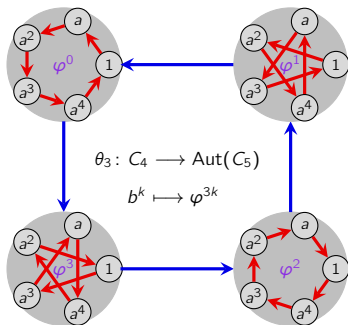
"labeling map"

$$C_4 \xrightarrow{\theta_3} \text{Aut}(C_5)$$

$$b^k \mapsto \varphi^{3k}$$

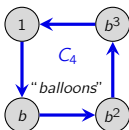
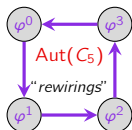


Stick in **rewired copies of A**, and then reconnect the **B-arrows**.



# An example: the direct product of $C_5$ and $C_4$

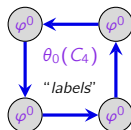
Let's now construct the "trivial" semidirect product,  $C_5 \rtimes_{\theta_0} C_4 = C_5 \times C_4$ :



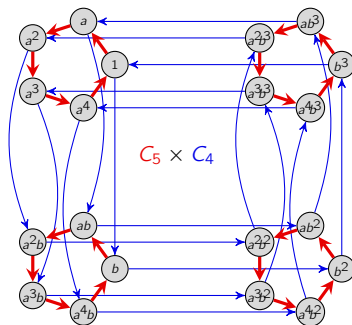
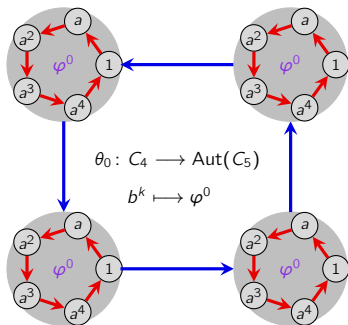
"labeling map"

$$C_4 \xrightarrow{\theta_0} \text{Aut}(C_5)$$

$$b^k \mapsto \varphi^0$$



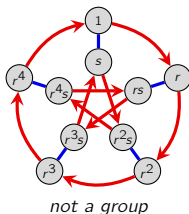
Stick in **rewired copies of A**, and then reconnect the **B-arrows**.



# Semidirect products

## Questions

- does our semidirect product construction actually yield a group?
- (what would happen if we try  $C_5$  and  $C_2$ ?)
- when do 2 labeling maps give isomorphic semidirect products?
- is the semidirect product commutative?



Which groups did we encounter when constructing  $C_5 \rtimes_{\theta_k} C_2$ , for  $k = 1, 2, 3$ ?

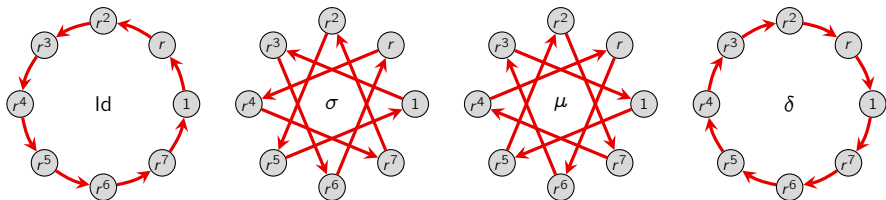
It turns out that there are only three nonabelian groups of order 20:

1. the **dihedral group**  $D_{10}$
2. the **dicyclic group**  $\text{Dic}_{10}$
3. a 1D "**affine group**"  $\text{AGL}_1(\mathbb{Z}_5) \cong \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \mathbb{Z}_5, a \neq 0 \right\} \leq \text{GL}_2(\mathbb{Z}_5)$ .

We'll answer these questions and more later, when we study automorphisms.

## Semidirect products of $C_8$ and $C_2$

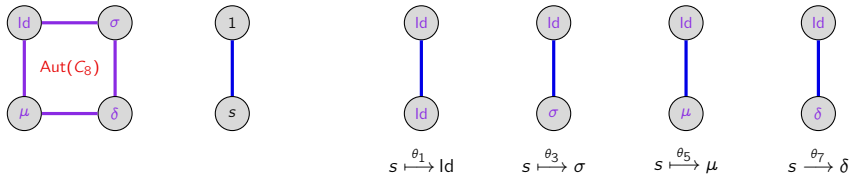
There are four rewirings of the Cayley diagram  $C_8 = \langle r \rangle$ :



All three non-trivial rewirings have order 2:

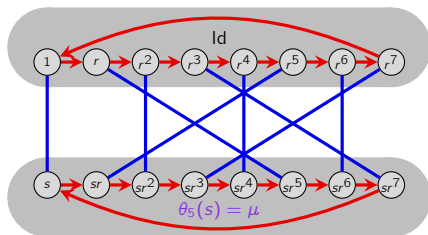
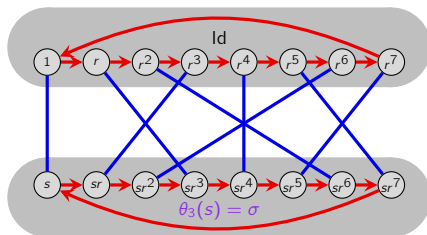
$$r \xrightarrow{\sigma} r^3 \xrightarrow{\sigma} (r^3)^3 = r^9 = r, \quad r \xrightarrow{\mu} r^5 \xrightarrow{\mu} (r^5)^5 = r^{25} = r, \quad r \xrightarrow{\delta} r^7 \xrightarrow{\delta} (r^7)^7 = r^{49} = r.$$

There are four nontrivial labeling maps  $\theta_k: C_2 \rightarrow \text{Aut}(C_8) \cong V_4$ :



## Semidirect products of $C_8$ and $C_2$

We know that  $C_8 \rtimes_{\theta_1} C_2 \cong C_8 \times C_2$  and  $C_8 \rtimes_{\theta_7} C_2 \cong D_8$ . Let's investigate the other two.



### Theorem

For each  $n = 2^m$ , there are four distinct semidirect products of  $C_n$  with  $C_2$ :

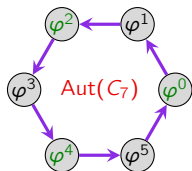
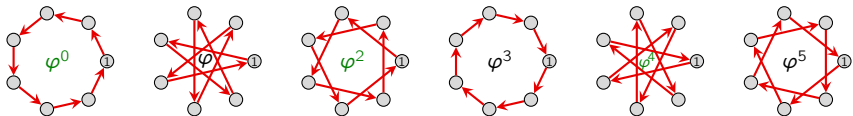
- $C_n \rtimes_{\theta_1} C_2 \cong C_n \times C_2$ ,
- $C_n \rtimes_{\theta_\sigma} C_2 \cong SD_n$ ,
- $C_n \rtimes_{\theta_\mu} C_2 \cong SA_n$ ,
- $C_n \rtimes_{\theta_\delta} C_2 \cong D_n$ ,

where the rewirings are maps  $C_{2^m} \rightarrow C_{2^m}$  defined by

$$r \xrightarrow{\theta_1} r, \quad r \xrightarrow{\theta_\sigma} r^{2^{m-1}-1}, \quad r \xrightarrow{\theta_\mu} r^{2^{m-1}+1}, \quad r \xrightarrow{\theta_\delta} r^{-1}.$$

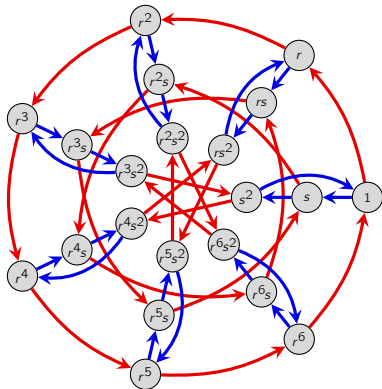
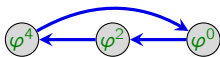
# The smallest nonabelian group of odd order: $C_7 \rtimes_{\theta} C_3$

There are 6 re-wirings (automorphisms) of  $C_7$ :



$$C_3 \xrightarrow{\theta} \text{Aut}(C_7)$$

$$s^k \mapsto \varphi^{2^k}$$



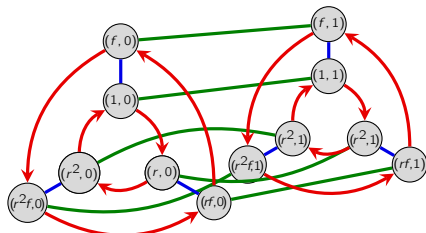
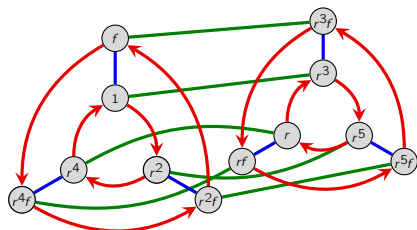
## A surprising fact

We know that we can construct the dihedral group  $D_6$  as a semidirect product  $C_6 \rtimes_{\theta} C_2$ .

But it also secretly decomposes as a *direct product*!

To see this, let's draw a Cayley diagram with a nonstandard generating set,

$$D_6 = \langle r^2, r^3, f \rangle.$$



It is apparent that  $D_6 \cong D_3 \times \mathbb{Z}_2 = \langle (r, 0), (f, 0), (0, 1) \rangle!$

**Question:** How does this generalize to larger dihedral groups?

We'll understand this better later when we study subgroups.

## Groups of matrices

We have already seen how many familiar groups can be represented by matrices.

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

Let's define a few terms so we can better speak of certain sets of matrices.

Square matrices are examples of objects where we can **add**, **subtract**, and **multiply**, but not always divide.

### Definition

A **ring** is an abelian group  $R$  that is additionally

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

The set  $\text{Mat}_{n,m}(R)$  of  $n \times m$  matrices is a group under addition, but a very boring one.

It is isomorphic to the direct product  $R^{mn} := R \times \cdots \times R$  of  $nm$  copies of  $R$ .

It is more interesting to look at groups of square matrices under multiplication.

### Definition

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



## Groups of matrices

Some rings contain **zero divisors**: two nonzero  $x, y$  such that  $xy = 0$ .

For example,  $2 \cdot 3 = 0$  in  $\mathbb{Z}_6$ .

In other rings, multiplication does not commute.

Henceforth, we will assume that our set of coefficients  $R$  is a **commutative ring** without zero divisors.

Basically, we're interested in examples like  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $\mathbb{Z}_n$ , etc.

Since matrices represent linear transformation, many standard matrix groups have "*linear*" in their names.

### Definition

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

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

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

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

## An interesting group of order 24

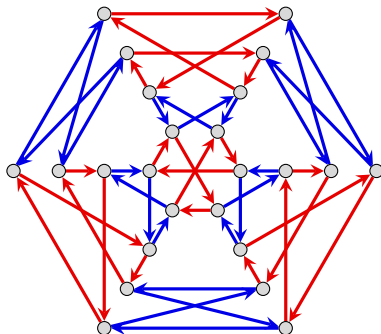
Some interesting finite groups arise as special or general linear groups over  $\mathbb{Z}_q$ . For example,

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

and the matrices  $A$  and  $B$  can be taken to be

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

Here's a Cayley diagram for different generators:  $\mathrm{SL}_2(\mathbb{Z}_3) = \langle R, S \mid R^6 = S^4 = (RS)^3 = I \rangle$ .



## The Hamiltonians

The group  $SL_2(\mathbb{Z}_3)$  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  $2 \times 2$  matrices over  $\mathbb{C}$ :

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

Yet another way involves  $4 \times 4$  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 associate with points in a 3-sphere:

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

The special linear group  $SL_2(\mathbb{Z}_3)$  can be realized as a particular subgroup,

$$SL_2(\mathbb{Z}_3) \cong \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k) \right\} \leq S^3.$$

## Matrix groups over other finite fields

The group  $\mathrm{GL}_n(\mathbb{Z}_p)$  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,

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

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

For example, by “dumb luck”,

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

## 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 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  $p^3$ .** Starting 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  $\mathbb{Z}_p$ ,

$$\text{Heis}(\mathbb{Z}_p) := \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{Z}_p \right\},$$

- 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**:

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

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

## The diquaternion group

Recall our standard representations of the quaternion and dihedral groups:

$$Q_8 = \langle i, j, k \rangle \cong \left\langle \underbrace{\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}}_{R=R_4}, \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_S, \underbrace{\begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}}_{T=RS} \right\rangle, \quad D_n = \langle r, f \rangle \cong \left\langle \underbrace{\begin{bmatrix} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{bmatrix}}_{R_n}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_F \right\rangle.$$

Now, 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**

$$DQ_8 = \langle X, Y, Z \rangle = \{ \pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ \},$$

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

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

It is easy to check that

$$XY = R \quad "i", \quad XZ = S \quad "j", \quad YZ = \bar{T} \quad "k".$$

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"**  $\text{Pauli}_1 = C_4 \circ D_4$ .



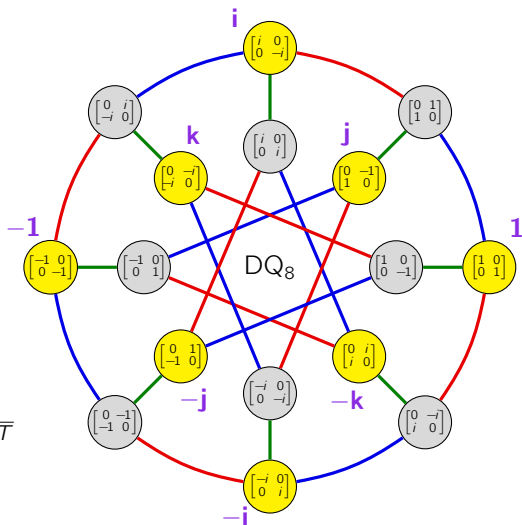
# The diquaternion group

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

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

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

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



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**

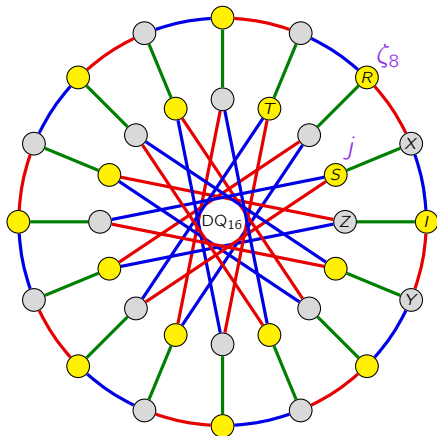
$$DQ_n := \langle \underbrace{\begin{bmatrix} \zeta_n & 0 \\ 0 & \bar{\zeta}_n \end{bmatrix}}_{R=R_n}, \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_S, \underbrace{\begin{bmatrix} 0 & -\zeta_n \\ \bar{\zeta}_n & 0 \end{bmatrix}}_{T=T_n}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_F \rangle \cong \text{Dic}_n \rtimes_{\theta} C_2.$$

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

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

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

$$XY_8 = R_8, \quad XZ = S, \quad Y_8Z = \bar{T}_8$$



# Groups of order $\leq 30$

| 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         | $C_{16}$            |            | $D_{10}$                     |            | $C_{25}$            |
| 6     | $C_6$            |            | $C_8 \times C_2$    |            | $\text{Dic}_{10}$            | 26         | $C_5 \times C_5$    |
|       | $D_3$            |            | $C_4^2$             |            | $\text{AGL}_1(\mathbb{Z}_5)$ |            | $C_{26}$            |
| 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         | $C_{22}$                     |            | $C_9 \times C_3$    |
|       | $C_2^3$          |            | $\text{SD}_8$       |            | $D_{22}$                     |            | $C_3^3$             |
|       | $D_4$            |            | $\text{SA}_8$       | 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    | $C_{10}$         |            | $C_4 \rtimes C_4$   |            | $D_{12}$                     |            | $D_{14}$            |
|       | $C_5 \times C_2$ |            | $C_2^2 \rtimes C_4$ |            | $\text{Dic}_{12}$            |            | $\text{Dic}_{14}$   |
| 11    | $C_{11}$         |            | $\text{DQ}_8$       |            | $S_4$                        | 29         | $C_{29}$            |
| 12    | $C_{12}$         | 17         | $C_{17}$            |            | $\text{SL}_2(\mathbb{Z}_3)$  | 30         | $C_{30}$            |
|       | $C_6 \times C_2$ | 18         | $C_{18}$            |            | $A_4 \times C_2$             |            | $D_{15}$            |
|       | $D_6$            |            | $C_6 \times C_3$    |            | $\text{Dic}_{12} \times C_2$ |            | $D_5 \times C_3$    |
|       | $\text{Dic}_6$   |            | $D_9$               |            | $D_4 \times C_3$             |            | $D_3 \times C_5$    |

The number of groups of order  $n$  is...

1009. 1

1010. 6

1011. 2

1012. 13

1013. 1

1014. 23

1015. 2

1016. 12

1017. 2

1018. 2

1019. 1

1020. 37

1021. 1

1022. 4

1023. 2

1024. 49,487,365,422

The number of  $p$ -groups, for  $p = 2, 3, 5$  is. . .

|       |                |       |         |         |         |
|-------|----------------|-------|---------|---------|---------|
| 2.    | 1              | 3.    | 1       | 5.      | 1       |
| 4.    | 2              | 9.    | 2       | 25.     | 2       |
| 8.    | 5              | 27.   | 5       | 125.    | 5       |
| 16.   | 14             | 81.   | 15      | 625.    | 15      |
| 32.   | 51             | 243.  | 67      | 3125.   | 77      |
| 64.   | 267            | 729.  | 504     | 15625.  | 684     |
| 128.  | 2,328          | 2187. | 9,310   | 78125.  | 34,297  |
| 256.  | 56,092         | 6561. | unknown | 390625. | unknown |
| 512.  | 10,494,213     |       |         |         |         |
| 1024. | 49,487,365,422 |       |         |         |         |
| 2048. | unknown        |       |         |         |         |

*“The human race will never know the exact number of groups of order 2048.”*  
–John Conway (Princeton University)

## Almost all finite groups are 2-groups

### Amazing fact

There are 49,910,529,415 groups of order  $|G| \leq 2000$ .

Of these, 49,487,365,422 of them (99.2%!) have order 1024

### Conjecture

Almost all finite groups are 2-groups. That is,

$$\lim_{n \rightarrow \infty} \frac{\# \text{ 2-groups groups of order } \leq n}{\# \text{ of groups of order } \leq n} = 1.$$

A few fun resources for exploring finite groups include:

- The interactive GroupExplorer website (only small groups):

*<https://nathancarter.github.io/group-explorer/index.html>*

- The noninteractive **GroupNames** website (comprehensive list):

*[people.maths.bris.ac.uk/~matyd/GroupNames/index.html](http://people.maths.bris.ac.uk/~matyd/GroupNames/index.html)*