Week 2

Group Theory Foundations

2.1 Groups of Low Order

10/3:

- Calegari: Nothing in particular to know for missing Friday; Adi will get me notes.
- Having explored examples, today, we're coming back down to earth to flex our axiomatic muscles.
- Distinguishing sets and binary operations.

Group	G	$*$	?
S_n	shuffles	composition	cards
$\mathrm{O}(n)$ and $\mathrm{SO}(n)$	(sp) orthogonal matrices	composition	vectors?
$\mathbb{Z}$	integers	addition	
$\mathbb{Z}/n\mathbb{Z}$	$\{0,1,\dots,n-1\}$	addition modulo n	

Table 2.1: Elements of a group.

  - Be careful not to confuse the shuffles and the cards; the cards are something else curious but are *not* the elements of the group.
  - Notice that $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are **commutative** groups, but the shuffles (for $n>1$) and $\mathrm{O}(n)$ are not.
  - Note that S_2, $\mathrm{O}(1)$, and $\mathbb{Z}/2\mathbb{Z}$ are all isomorphic groups.
- **Commutative** (group): A group such that for all $x,y\in G$, $x*y=y*x$. *Also known as* **Abelian**.
- Lemma (Cancellation Lemma): Let $x,y,z\in G$. Then $xy=xz$ implies $y=z$ and $yx=zx$ implies $y=z$.

Proof. We have that

$$\begin{aligned} x*y &= x*z \\ x^{-1}*(x*y) &= x^{-1}*(x*z) && \text{Inverses exist} \\ (x^{-1}*x)*y &= (x^{-1}*x)*z && \text{Associativity} \\ e*y &= e*z \\ y &= z \end{aligned}$$

as desired.

The proof of the second statement is symmetric. □

  - This will be Calegari's only proof from the axioms directly.

- **Multiplication table** (for G): A table with all elements of G on the top and the side, and all binary products in it.
  - The total number of binary operations is n^{n^2}?
  - To check that a group is a group, we can write out its multiplication table and confirm pointwise that the group axioms are satisfied. However, there are also many ways to speed this process up.
  - An example of a multiplication table can be found on the right in Figure 2.1.
- **Trivial group**: The only group with $|G| = 1$, i.e., $G = \{e\}$.
- A group of $|G| = 2$ has the form $G = \{e, x\}$ where we must have $x = x^{-1}$.
  - We can find this by inspection or invoke the **Sudoku Lemma**.
  - Thus, all groups of order 2 are isomorphic.
- Lemma (Sudoku Lemma): Fix $x \in G$. Then

  $$\{xg \mid g \in G\} = G = \{gx \mid g \in G\}$$

  Proof. There exists g such that $xg = y$ for x, y fixed: Choose $g = x^{-1}y$.

  y only occurs once: If $xg = y$ and $xg' = y$, transitivity and the cancellation lemma imply $g = g'$. □

  - In layman's terms, in every row and column of the multiplication table, each element of G occurs exactly once.
- Playing Sudoku, we can show that all groups of order 3 are isomorphic.

	e	x	y
e	e	x	y
x	x		
y	y		

$\longrightarrow$

	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Figure 2.1: Playing Sudoku for $|G| = 3$.

  - Start from the left table above.
  - Notice that row 3 has a y and column 2 has an x, so by the Sudoku Lemma, e must be the element in row 3, column 2.
  - Then column 2 has e, x in it, so the entry in row 2, column 2 must by y.
  - Then row 2 has x, y in it, so the entry in row 2, column 3 must be e.
  - Then row/column 3 both have e, y in them, so the entry in row 3, column 3 must be x.
- However, we cannot play Sudoku in the same way with groups of order 4. In fact, there are multiple groups of order 4.
  - Two cases: (1) $x^2 \neq e$ so WLOG let $x^2 = y$, and (2) $a^2 = e$ for $a = x, y, z$.
    - Case 1 is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.
    - Case 2 is isomorphic to the **direct product** of $\mathbb{Z}/2\mathbb{Z}$ with itself, also known as the **Klein 4-group**.
  - This should not come as a surprise: We've already encountered the very different groups S_4 and $\mathbb{Z}/24\mathbb{Z}$ of order 24.

- **Direct product**: The group whose set is the Cartesian product of the sets of groups $A = (A, *_A), B = (B, *_B)$, and whose operation is coordinate-wise multiplication. *Given by*

$$G = A \times B \qquad\qquad (a, b) *_G (a', b') = (a *_A a', b *_B b')$$

  - We can prove that $e = (e_A, e_B)$, that $(a, b)^{-1} = (a^{-1}, b^{-1})$, and that associativity holds.
  - We have that

$$|G| = |A| \cdot |B|$$

- There is only one group of order 5.
- Examples of groups of order 6: S_3, $\mathbb{Z}/6\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
  - Are there any two groups which are distinct?
    - S_3 is not commutative, but the others are, so it is distinct from them.
    - $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ and $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ are the same because order doesn't matter in the construction of the direct product.
    - $\mathbb{Z}/6\mathbb{Z}$ and the two direct products are the same because they both have elements of order 6 (i.e., a one-element generator). The cycles are:

$$\begin{aligned}
1^1 &= 1 &&= 1 & \qquad (1,1)^1 &= (1,1) &&= (1,1)\\
1^2 &= 1+1 &&= 2 & (1,1)^2 &= (1+1, 1+1) &&= (2,0)\\
1^3 &= 2+1 &&= 3 & (1,1)^3 &= (2+1, 0+1) &&= (0,1)\\
1^4 &= 3+1 &&= 4 & (1,1)^4 &= (0+1, 1+1) &&= (1,0)\\
1^5 &= 4+1 &&= 5 & (1,1)^5 &= (1+1, 0+1) &&= (2,1)\\
1^6 &= 5+1 &&= 0 & (1,1)^6 &= (2+1, 1+1) &&= (0,0)\\
1^7 &= 0+1 &&= 1 & (1,1)^7 &= (0+1, 0+1) &&= (1,1)
\end{aligned}$$

  - These are the only two groups of order 6.
- Continuing on, there is only 1 group with $|G| = 2047$ (which is "mostly prime" — connection between primes and number of groups?), but there are 1,774,274,116,992,170 groups of $|G| = 2048 = 2^{11}$.
- Conclusion: The arithmetic of $|G|$ has an impact on the structure of G.

2.2 The Symmetric Group

10/5:

- **Symmetric group** (on n letters): The set of all bijections from the set of numbers $\{1, \dots, n\}$ to itself, whose operation is function composition. *Denoted by* $\boldsymbol{S_n}$.
  - Convention: Denote elements of S_n not by f but by σ, τ.
  - $\sigma\tau$ means do τ first and then σ.
  - $|S_n| = n!$.
- One of the first challenges we encounter when defining new objects is a notational one.
  - We could define a function with a table, but cycle notation is easier.
- ***k*-cycle**: The bijection

$$m \mapsto \begin{cases} a_{i+1} & m = a_i,\ i \neq k\\ a_1 & m = a_k\\ m & m \neq a_i \end{cases}$$

in S_n, where $a_1, \dots, a_k$ are distinct elements of $[n]$. *Denoted by* $\boldsymbol{(a_1, a_2, \dots, a_k)}$.

  - If σ is a k-cycle, then the order of σ is k.
  - There are k ways to write down the same k-cycle.
    - For example, $(i,j)=(j,i)$ and $(a,b,c)=(b,c,a)=(c,a,b)$.
  - All 1-cycles are the identity e.
  - Combinatorics: How many k-cycles are there in S_n?
    - $k=1$: Just one – (e).
    - $k=2$: $\binom{n}{2}$.
    - $k=3$: $\binom{n}{3}\cdot 2$.
      - We must first choose 3 of the n possible elements to be manipulated by the k-cycle.
      - But then we can send a_1 to a_2 or a_3, so that's an additional two choices beyond just a selection of 3 elements. Once we send a_1 to a_2 or a_3, the rest of the cycle is determined, so we need not augment any more.
    - k: $\binom{n}{k}\cdot(k-1)! = \frac{n!}{(n-k)!k}$.
      - As before, we must choose k of the n possible elements to be manipulated by the k-cycle.
      - However, here, there are $k-1$ possibilities to which we can send a_1, so we need to multiply by that. Once we've determined $\sigma(a_1)$, there are $k-2$ possibilities to which we can send $\sigma(a_1)$. This pattern naturally continues, and we end up needing to correct $\binom{n}{k}$ by $(k-1)!$.

- Proposition: Every $\sigma\in S_n$ can be written as a product/composition of disjoint cycles. Moreover, disjoint cycles commute.

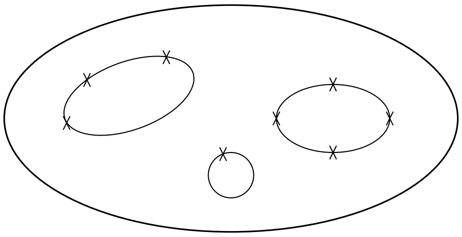

Figure 2.2: Decomposing σ into disjoint cycles.

  - The idea behind this proposition is that every element will cycle back to itself eventually, and you can't get to elements of one cycle if you're not in the cycle (so all cycles are disjoint).
  - Every permutation can be visualized by ordering the n letters in a set in $\mathbb{R}^2$ and connecting all disjoint cycles (think a circle full of oriented circles/loops/cycles).

- Composing cycles. See what the right one does and then the left one. Canonically, start with 1.
- Proposition: The cycle decomposition of σ is unique up to...
  - The ordering of the disjoint cycles;
  - Cycle permutations of each cycle;
  - Include/exclude 1-cycles.

  Moreover, $|\sigma|$ is the least common multiple of the cycle lengths.

- How many elements in S_6 have a cycle shape that looks like $(x,x)(x,x)(x,x)$?
  - It is
$$\frac{6!}{2^3\cdot 3!}=15$$
  - Rationale: See PSet 2, Q1a.

- The cycle decompositions of all elements in S_4.

$(1,2,3,4)$	$(1,2,3)$	$(1,2)$	$(1,2)(3,4)$	e
$(1,2,4,3)$	$(1,3,2)$	$(1,3)$	$(1,3)(2,4)$	
$(1,3,2,4)$	$(1,2,4)$	$(1,4)$	$(1,4)(2,3)$	
$(1,3,4,2)$	$(1,4,2)$	$(2,3)$		
$(1,4,2,3)$	$(1,3,4)$	$(2,4)$		
$(1,4,3,2)$	$(1,4,3)$			
	$(2,3,4)$			
	$(2,4,3)$			

Table 2.2: S_4 cycle decompositions.

- **Conjugate** (elements x,y): Two elements $x,y \in G$ a group for which there exists $g \in G$ such that $y = g \cdot x \cdot g^{-1}$. *Denoted by* $\boldsymbol{x \sim y}$.
- Lemma: Conjugacy is an equivalence relation.
  - (I) $x \sim x$.

    Proof. $x = exe^{-1}$. □
  - (II) If $y \sim x$, then $x \sim y$.

    Proof. Take
    $$\begin{aligned} y &= gxg^{-1} \\ g^{-1}y(g^{-1})^{-1} &= x \end{aligned}$$
    □
  - (III) If $x \sim y$ and $y \sim z$, then $x \sim z$.

    Proof. Suppose $y = gxg^{-1}$ and $z = hyh^{-1}$. Then
    $$z = hgxg^{-1}h^{-1} = (hg)x(hg)^{-1}$$
    □
- **Conjugacy class** (of x): A subset of G containing all $g \in G$ which are conjugate to a certain $x \in G$. *Denoted by* $\boldsymbol{C(x)}$. *Given by*
  $$C(x) = \{g \in G \mid g \sim x\}$$
- Straightforward: Not necessarily obvious, but there's nothing really tricky going on.
  - The joke about the mathematician who says something is obvious, someone asks why?, he thinks for 20 minutes, and then says it's obvious.
- Why is conjugacy important?
  - In linear algebra, we've seen it with similar matrices.
    - Same linear map in a different basis is the same as conjugating the matrix of the map in one basis with the change of basis matrix.
  - Conjugacy tells us that a set of objects are, in some way, the same.

2.3 Blog Post: The Symmetric Group

From Calegari (2022).

10/24:
- Relevant section from Dummit and Foote (2004): 1.3.
- Review from class plus more details on the riffle shuffle problem.

2.4 Conjugacy

10/7:
- You can request one extension per quarter on homework (possibly more if you have a really good reason) for sickness, etc., no questions asked. Email your TA to secure this extension.
- Last time, we began covering conjugacy.
  - Conjugacy classes.
  - Conjugacy defines an equivalence relation on G.
  - $G = \bigsqcup$ conjugacy classes[1].
- More on conjugacy today.
- The conjugacy class of e is $\{e\}$.
- If $y = gxg^{-1}$, then $y^k = gx^kg^{-1}$.
- Proposition: $y \sim x$ implies $|y| = |x|$.

  Proof. Suppose $|y| = k$, i.e., $y^k = e$. By the above statement, we know that $y^k \sim x^k$. Since $y^k = e$, it follows that $e \sim x^k$. Thus, x^k is in the conjugacy class of e. But since the conjugacy class of e is $\{e\}$, this means that $x^k = e$, as desired. □

- Conjugacy in S_n, $n \geq 2$.
  - Each $x \in S^n$ has a cycle decomposition
  $$x = (a_1, \dots, a_k)(b_1, \dots, b_m)(c_1, \dots) \cdots$$
  - We want to investigate the properties of gxg^{-1} for an arbitrary $g \in S_n$. Ideally, we'd like to express it in a form related to x.
  - Trick: Apply gxg^{-1} to $g(a_1)$. Then
  $$gxg^{-1}(g(a_1)) = gx(a_1) = g(a_2)$$
  - It follows by induction that
  $$gxg^{-1} = (g(a_1), \dots, g(a_k))(g(b_1), \dots, g(b_m))(g(c_1), \dots) \cdots$$
  - Now suppose that $m \neq g(a_i), g(b_j), g(c_k), \dots$. Then
  $$g^{-1}(m) \notin \{a_1, \dots, a_k, b_1, \dots, b_m, c_1, \dots\}$$

    It follows since x is the identity on such elements that $x(g^{-1}(m)) = g^{-1}(m)$. Therefore, since all functions involved are bijections,
  $$[gxg^{-1}](m) = g[x(g^{-1}(m))] = g(g^{-1}(m)) = m$$

[1] $\bigsqcup$ denotes a **disjoint union**. Think of the *disjoint* union of sets as a union of sets that happen to be disjoint, the same way a *direct* sum of subspaces is a sum of subspaces that happen to be linearly independent.

  - It follows that gxg^{-1} has the same **cycle shape**.

- **Shape** (of $g \in S_n$): The partition of n given by the lengths of the cycles in the cycle decomposition of g in decreasing order. *Also known as* **cycle shape**, **partition**.

S_4	4-cycle	3-cycle	Product of 2-cycles	1-cycles
Cycle decomposition	(x,x,x,x)	$(x,x,x)(x)$	$(x,x)(x,x)$	$(x)(x)(x)(x)$
Shape	4	$3+1$	$2+2$	$1+1+1+1$

Table 2.3: Shape of elements in S_4.

- Claim: $x, y \in S_n$ are conjugate iff they have the same cycle shape.

  Proof. We will do a proof by example that illustrates the idea of the generalized proof.

  Let

$$x = (1,2,3)(4,5,6)(7,10) \qquad\qquad y = (2,3)(4,1,5)(6,9,10)$$

  Note that both have the same cycle shape: $3+3+2+1+1$. We now use a two-step process to define a g such that $y = gxg^{-1}$.

  Step 1: Including 1-cycles, line both x and y up so they "match."

x	$(\ 1$	2	$3\ )$	$(\ 4$	5	$6\ )$	$(\ 7$	$10\ )$	$(\ 8\ )$	$(\ 9\ )$
y	$(\ 4$	1	$5\ )$	$(\ 6$	9	$10\ )$	$(\ 2$	$3\ )$	$(\ 7\ )$	$(\ 8\ )$
gxg^{-1}	$(g(1)$	$g(2)$	$g(3))$	$(g(4)$	$g(5)$	$g(6))$	$(g(7)$	$g(10))$	$(g(8))$	$(g(9))$

  Step 2: We want $y = gxg^{-1}$. Thus, take g to be the map which sends every entry in gxg^{-1} to the entry of y directly above it. For example, we want $g(1) = 4$, $g(2) = 1$, $g(3) = 5$, ... Noting that $g(1) = 4$, $g(4) = 6$, $g(6) = 10$, ..., we realize that g can actually be written as the following cycle.

$$g = (1,4,6,10,3,5,9,8,7,2)$$

□

- Follow ups.
  - How many different g's satisfy $y = gxg^{-1}$?
    - Depends on the number of ways y can be matched up with x.
    - The above manner obviously works.
    - However, we can rotate the elements in both 3-cycles three ways, and the elements of the 2-cycle two ways, so that's $3 \cdot 3 \cdot 2 = 18$ g's right there.
    - Additionally, we can swap the place of the 3-cycles and the 1-cycles entirely, so thats an additional $2 \cdot 2$ times as many ways.
    - All told, there are $3 \cdot 3 \cdot 2 \cdot 2 \cdot 2 = 72$ possible g's.
    - See HW2, Q1a for a treatment of an analogous problem.
  - Counting the size of conjugacy classes.
    - Suppose G is an abelian group. Then if $y = gxg^{-1}$, $y = gg^{-1}x = x$, so the size of the conjugacy class of any $x \in G$ is 1.
    - For this reason, the elements of $\mathbb{Z}/n\mathbb{Z}$ and of SO(2) are conjugate only to themselves.
    - However, we get something different for O(2). Here, we can prove that the conjugacy class of every rotation r is $\{r, r^{-1}\}$, and that all reflections are in the same conjugacy class[2].

[2] This is fundamentally related to the structure of point groups in inorganic chemistry! Remember that in C_{5v}, for instance, C_5, C_5^4 are conjugate, C_5^2, C_5^3 are conjugate, and all reflections get lumped together.

  - Let r denote a rotation, and s denote a reflection.
  - Suppose $x = r$. Then

$$\begin{aligned} e &= (sr)^2 \\ &= srsr \\ r^{-1} &= srs \\ &= srs^{-1} \end{aligned}$$

  where we have HW1, Q2d(i) to justify the first equality and the fact that every reflection is it's own inverse[3] to justify the last equality.

  - On the other hand, suppose $x = s$. Then if r is any rotation,

$$\begin{aligned} srsr &= e \\ rsr &= s^{-1} \\ rsrr^{-2} &= s^{-1}r^{-2} \\ rsr^{-1} &= sr' \end{aligned}$$

  where r' denotes r^{-2} to express the main takeaway: that s is conjugate to itself times any rotation (for r' arbitrary, we may choose $r = (r')^2$). In other words, since all reflections are related by some rotation, all reflections are, indeed, in the same conjugacy class.

- Generators of S_n, $n \geq 3$.
- Lemma: The set of 2-cycles generates S_n.

Proof. It only requires $n - 1$ swaps between pairs of elements to get to any permutation. For example, to get to

$$\begin{array}{ccc} 1 & & 3 \\ 2 & \mapsto & 4 \\ 3 & & 2 \\ 4 & & 1 \end{array}$$

we can swap 1 and 3 (so $1 \mapsto 3$), then 2 and 4 (so $2 \mapsto 4$), then "3" and "4" (so $3 \mapsto 2$ and $4 \mapsto 1$). More graphically,

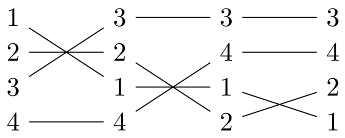

Figure 2.3: Generating S_n with 2-cycles.

The idea is we fix the first element and then work down the list. □

- S_n is also generated by

$$\{(1,2),(2,3),(3,4),\dots,(n-1,n)\} \qquad \{(1,2),(1,3),(1,4),\dots,(1,n)\}$$

  - Both of these sets have cardinality $n - 1$.

- As we can see from the above...

[3] Intuitively, applying any reflection twice yields the original object.

  - If we generate S_n with all 2-cycles, the generator set has cardinality $\frac{n}{2}(n-1)$;
  - If we generate S_n with all elementary 2-cycles, the generator set has cardinality $n-1$.
- But we can do even better: Let $\sigma=(1,2)$ and $\tau=(1,2,\dots,n)$. Then any

$$(k,k+1)=\tau^{k-1}\sigma\tau^{-(k-1)}$$

  - Indeed, we can see that using the RHS above, $k\mapsto 1\mapsto 2\mapsto k+1$ and $k+1\mapsto 2\mapsto 1\mapsto k$. Every other element receives the identity treatment, as we can confirm.

2.5 Blog Post: Conjugacy

From Calegari (2022).

10/22:

- x,y are conjugate implies $|x|=|y|$, but $|x|=|y|$ does not imply x,y are conjugate.
  - Example: $(1,2)$ and $(1,2)(3,4)$ in S_4 are not conjugate (their cycle shapes differ) but they are both of order 2.
- $\boldsymbol{p(n)}$: The number of possible partitions of $\sigma\in S_n$.
- Growth rate of $|n|$ and $p(n)$.
  - We have

$$p(n)\sim\frac{1}{4n\sqrt{3}}\exp\left(\pi\sqrt{\frac{2n}{3}}\right)$$

    - ~ means that the ratio of the two numbers converges to 1 as $n\to\infty$.
  - We also have that

$$|n|=n!\sim n^n\mathrm{e}^{-n}\sqrt{2\pi n}$$

  - Since

$$\log n!\sim n\log n \qquad\qquad \log p(n)\sim Cn^{1/2}$$

    for some explicit C, we know that $|n|$ grows much faster than $p(n)$.

2.6 Chapter 1: Introduction to Groups

From Dummit and Foote (2004).

Dihedral Groups

12/5:

- **Dihedral group**: A group whose elements are symmetries of regular planar figures.
- D_{2n} denotes the group of symmetries of a regular n-gon for $n\geq 3$.
- **Symmetry**: Any rigid motion which can be effected by taking a copy of a shape, moving this copy in any fashion in 3 space, and then placing the copy back on the original so that it exactly covers it.
- Describe symmetries mathematically by labeling the vertices of a regular n-gon from $1,\dots,n$ and mapping each symmetry s to the unique corresponding permutation σ of $\{1,\dots,n\}$.
  - Make it a group by letting function composition be the group operation. (Function composition is naturally associative.)
- Note that $|D_{2n}|=2n$.

  - "Since symmetries are rigid motions, one sees that once the position of the ordered pair of vertices 1,2 has been specified, the action of the symmetry on all remaining vertices is completely determined" (Dummit & Foote, 2004, p. 24).
  - Thus, there are $n \cdot 2$ possible rigid motions (sending vertex one to any of the n options, and then vertex two to one of the 2 adjacent positions).

- The elements of D_{2n} are the n rotations by $2\pi i/n$ about the center of the n-gon, and the n reflections about the n lines of symmetry (which may come in one type or two; see Figure 3.2).

- Abstracting D_{2n}: Fix a regular n-gon centered at the origin in the xy-plane and label the vertices consecutively from 1 to n in a clockwise manner. Let r be the rotation clockwise about the origin through $2\pi/n$ radians. Let s be the reflection about the line of symmetry through vertex 1 and the origin. Then

  1. $1, r, r^2, \dots, r^{n-1}$ are distinct and $r^n = 1$, so $|r| = n$.
  2. $|s| = 2$.
  3. $s \neq r^i$ for any i.
  4. $sr^i \neq sr^j$ for all $0 \leq i,\ j \leq n-1$ with $i \neq j$, so

     $$D_{2n} = \{1, \dots, r^{n-1}, s, \dots, sr^{n-1}\}$$

     In other words, each element of D_{2n} can be written uniquely in the form $s^k r^i$ for some $k = 0, 1$ and $0 \leq i \leq n-1$.
  5. $rs = sr^{-1}$. Thus, r, s do not commute so D_{2n} is non-abelian.
  6. $r^i s = sr^{-i}$ for all $0 \leq i \leq n$. This indicates how to commute s with powers of r.

- Relations (1), (2), and (6) allow us to simplify any product of two elements $s^{i_1} r^{i_2} s^{i_3} r^{i_4} \cdots$ to a product of the form $s^i r^j$.

- Note that r, s in the above example are **generators**, which will only be rigorously introduced later but are useful now and thus used informally.
  - Detailed discussion: Section 2.4. Rigorous treatment (with **free groups**): Section 6.3.

- **Generators** (of G): A subset $S \subset G$ with the property that every element in G can be written as a (finite) product of elements of S and their inverses.
  - We write $G = \langle S \rangle$ and say that "G is generated by S" or "S generates G."
  - Examples: $\mathbb{Z} = \langle 1 \rangle$ and $D_{2n} = \langle r, s \rangle$.
  - Later: We need not include the inverses of the elements of S as generators.

- **Relation** (in G): An equation in a general group G that the generators satisfy.
  - Example: In D_{2n}, we have $r^n = 1$, $s^2 = 1$, and $rs = sr^{-1}$. These relations have the additional property that *any* other relation may be deduced from them (since we can determine exactly when two group elements are equal using these), motivating the following.

- **Presentation** (of G): The set S of generators of G along with the relations $R_1, \dots, R_m$, where each R_i is an equation in the elements from $S \cup \{1\}$, such that any relation among the elements of S can be deduced from these. *Denoted by* $G = \langle \boldsymbol{S} \mid \boldsymbol{R_1, \dots, R_m} \rangle$.
  - Example: $D_{2n} = \left\langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \right\rangle$. This is far easier to work with than the motivating geometric description.
  - Limitations of presentations: It may be difficult (or impossible) to tell from a given presentation when two elements of the group are equal, what the order is, or even whether a group is finite or infinite.

- Dummit and Foote (2004) list examples and works with **collapsing** presentations, i.e., ones in which some important relations are consequences of others.
  - Dummit and Foote (2004) deduce that $X_{2n} = \left\langle x, y \mid x^n = y^2 = 1,\ xy = yx^2 \right\rangle$ has order at most 6, even though this is highly counterintuitive.
  - Groups with two generators and a relation $x^n = y^2 = 1$ have order *at most* $2n$, but may collapse much more, even down to the trivial group. D_{2n} has order $2n$ because we know by independent (geometric) means that such a group exists; finding such "lower bound" groups for other presentations can be much harder.
  - More on group presentations in Section 6.3.

Symmetric Groups

- **Symmetric group** (on the set Ω): The group $(S_\Omega, \circ)$, where S_Ω is the set of all bijections from a nonempty set Ω to itself and $\circ$ is function composition. *Also known as* **permutations** (of Ω).
  - We write $\sigma \in S_\Omega$ and let $1 \in S_\Omega$ be the identity function defined by $1(a) = a$ for all $a \in \Omega$.
  - If $\Omega = [n]$, then we denote S_Ω by S_n.
- **Symmetric group** (of degree n): The symmetric group on the set $\{1, 2, \dots, n\}$. *Denoted by* $\boldsymbol{S_n}$.
  - Section 1.6: The structure of S_Ω depends only on the cardinality of Ω, i.e., if $|\Omega| = n$, then S_Ω "looks like" S_n.
  - S_n will be studied in its own right and used to illustrate/motivate general group theory often throughout the text.
- $|S_n| = n!$.
  - Derivation for this presented as well.
- **Cycle**: A string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers).
  - The cycle $(a_1\ a_2\ \dots\ a_m)$ is the permutation which sends a_i to a_{i+1} for all $1 \leq i \leq m-1$ and sends a_m to a_1.
- **Cycle decomposition** (of σ): The product of all cycles describing part of the action of σ. *Given by*

$$(a_1\ a_2\ \dots\ a_{m_1})(a_{m_1+1}\ a_{m_1+2}\ \dots\ a_{m_2})\dots(a_{m_{k-1}+1}\ a_{m_{k-1}+2}\ \dots\ a_{m_k})$$

- Cycle decomposition algorithm (proof in Chapter 4):
  1. To start a new cycle, pick the smallest element of $[n]$ which has not yet appeared in a previous cycle — call it a (if you are just starting, choose $a = 1$); begin the new cycle: "$(a$".
  2. Read off $\sigma(a)$ from the given description of σ — call it b. If $b = a$, close the cycle with a right parenthesis (without writing b down); this completes a cycle — return to step 1. If $b \neq a$, write b next to a in this cycle: "$(a\ b$".
  3. Read off $\sigma(b)$ from the given description of σ — call it c. If $c = a$, close the cycle with a right parenthesis to complete the cycle — return to step 1. If $c \neq a$, write c next to b in this cycle: "$(a\ b\ c$". Repeat this step using the number c as the new value for b until the cycle closes.
  4. Remove all cycles of **length** 1.

- Example:

$$\begin{array}{llll} \sigma(1) = 12 & \sigma(2) = 2 & \sigma(3) = 3 & \sigma(4) = 1 \\ \sigma(5) = 11 & \sigma(6) = 9 & \sigma(7) = 5 & \sigma(8) = 10 \\ \sigma(9) = 6 & \sigma(10) = 4 & \sigma(11) = 7 & \sigma(12) = 8 \end{array}$$

  becomes

$$\sigma = (1\ 12\ 8\ 10\ 4)(5\ 11\ 7)(6\ 9)$$

- **Length** (of a cycle): The number of integers which appear in it.
- ***t*-cycle**: A cycle of length t.
- **Disjoint** (cycles): Two cycles that have no numbers in common.
- The convention of removing all cycles of length 1 makes it so that any cyclic decomposition essentially represents a bijection on the infinite set $\mathbb{N}$, not just $[n]$; in particular, σ can be though of as a function $\sigma : \mathbb{N} \to \mathbb{N}$.
  - Thus, $\sigma \in S_n$ is represented by the same cycle decomposition when it's an element of S_m, $m \geq n$.
  - The cycle decomposition for the identity element of S_n is taken to be 1.
- For any $\sigma \in S_n$, the cyclic decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order.
  - Continuing with the above example, $\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(7\ 11\ 5)(9\ 6)$.
- Dummit and Foote (2004) covers computing products of cycle decompositions.
- S_n is a non-abelian group for all $n \geq 3$.
- Disjoint cycles commute.
- We can permute the disjoint cycles in a cycle decomposition and rotate (cyclically permute) the elements of a given cycle without affecting the identity of the cycle decomposition.
  - Convention: Smallest number written first in a cycle, and cycle containing the smallest number written first.
  - Thus, a cycle decomposition is "the *unique* way of expressing a permutation as a product of disjoint cycles (up to rearranging its cycles and cyclically permuting the numbers within each cycle)" (Dummit & Foote, 2004, p. 32).
- The order of a permutation is the l.c.m. of the lengths of the cycles in its cycle decomposition.