Groups

Combinatorics

Fall 2026

Many counting problems count objects up to some transformations. For example, we can ask how many ways there are to make a round bracelet with 10 beads, each black or red. Turning a bracelet does not change it, so two arrangements that differ by a rotation are the same bracelet. In Figure 13.1, reading the beads counterclockwise from the marked bead gives 3 black, 2 red, 2 black, 3 red on the left, and 1 black, 2 red, 2 black, 3 red, 2 black on the right; turning the left bracelet by two beads produces the right one.

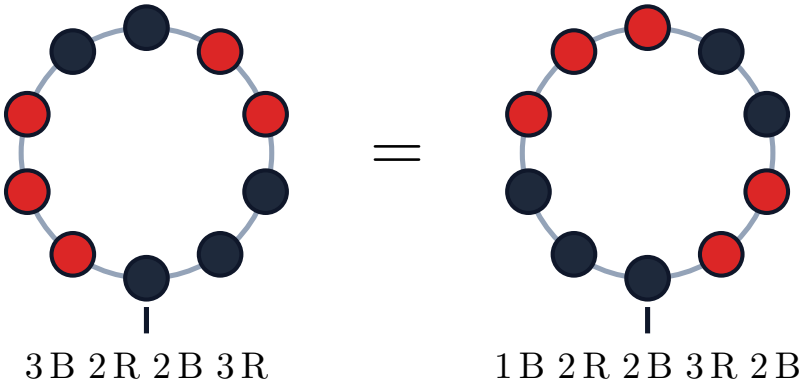

Figure 13.1: Two descriptions of the same bracelet with 10 beads. Reading counterclockwise from the marked bead gives 3B 2R 2B 3R on the left and 1B 2R 2B 3R 2B on the right. Turning the left bracelet by two beads gives the right one.

Figure description: Two rings of ten black and red beads joined by an equals sign, each with a tick below its bottom bead. Left ring, counterclockwise from the tick: 3 black, 2 red, 2 black, 3 red. Right ring: 1 black, 2 red, 2 black, 3 red, 2 black.

To count such quantities efficiently, we need a precise language for the transformations themselves. The algebraic notion that encodes transformations is called a **group**.

After studying these notes, you will be able to do the following.

- State what a group is, and recognize groups of transformations.
- Describe every symmetry of a regular n-gon as $r^j s^\varepsilon$, and compute products using the relations $r^n = s^2 = e$ and $sr = r^{-1}s$.
- Describe the symmetric group of permutations of n objects, and analyze the cycle structure of its elements.
- Explain what a presentation of a group is, and the difficulties involved in studying a group given by a presentation.
- Compose and invert permutations given by tables, and write permutations in cycle notation.
- Compose overlapping cycles, and compute conjugates of permutations by relabeling.
- Decide whether a subset of a finite group is a subgroup, and compute the order of an element.
- Find the cyclic subgroup generated by an element, relate its size to the order of the element, and decide whether a group is cyclic.

13.1 Coloring the corners of a square

We start with a smaller version of the bracelet problem, coloring the four corners of a square, and identify the properties of the rotations that the solution uses.

We label the corners of a square $1, 2, 3, 4$ counterclockwise, starting at the bottom left, and color each corner black or white. A coloring is recorded by the string $c(1)c(2)c(3)c(4)$ of the colors of corners $1, 2, 3, 4$; for example, `BWWW` colors corner 1 black and the other three corners white. Each of the four corners has two possible colors, so by the product rule there are $2^4 = 16$ colorings.

Suppose now that the square is a tile lying on a table, with its corners painted, and that the tile can be turned. Turning the tile by 90° counterclockwise carries the paint on corner 1 to the place of corner 2, the paint on corner 2 to the place of corner 3, the paint on corner 3 to the place of corner 4, and the paint on corner 4 to the place of corner 1. In terms of strings, each letter moves one place to the right and the last letter moves to the front: `BWWW` becomes `WBWW`. We regard two colorings as *the same up to rotation* if one of the four rotations, by 0°, 90°, 180°, or 270°, carries one coloring to the other.

To find all colorings that are the same as a given one, we apply the 90° rotation repeatedly until we return to the starting coloring. For example,

$$\texttt{BBWW} \to \texttt{WBBW} \to \texttt{WWBB} \to \texttt{BWWB} \to \texttt{BBWW}.$$

These four colorings form one class. Figure 13.2 sorts all 16 colorings into classes in this way.

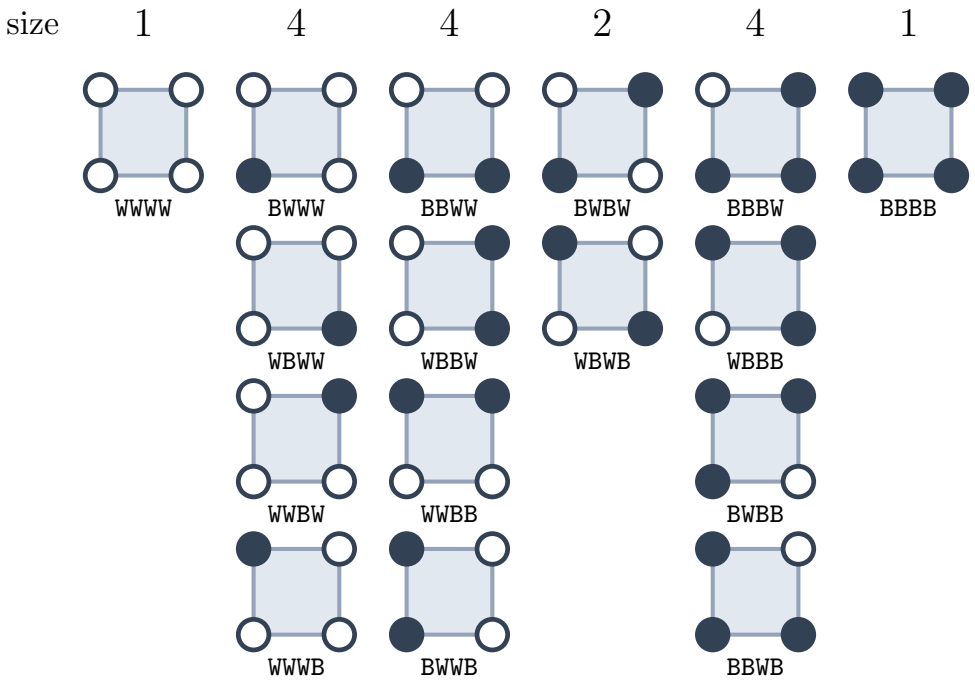

Figure 13.2: The 16 black-and-white colorings of the corners of a square, sorted into classes of colorings that are rotations of one another. Corner 1 is at the bottom left, and the corners continue counterclockwise. Going down a column turns the square by 90° counterclockwise. The number above each column is the size of the class.

Figure description: Six columns of small squares with black or white corners. Column sizes 1, 4, 4, 2, 4, 1: all white; one black corner; two adjacent black corners; two opposite black corners; three black corners; all black. Each square is labeled by its string, such as BBWW.

We describe the classes by the number of black corners.

- No black corners: `WWWW` is unchanged by every rotation, so its class has 1 coloring.
- One black corner: the black corner can be carried to any of the 4 corners, so the class has 4 colorings.
- Two black corners that are adjacent, that is, joined by a side: the black pair can be carried to any of the 4 sides, so the class has 4 colorings.
- Two black corners that are opposite: the black pair is one of the 2 diagonals. The half turn carries `BWBW` to itself, so the class has only 2 colorings.
- Three black corners: the white corner can be any of the 4 corners, so the class has 4 colorings.
- Four black corners: `BBBB` is unchanged by every rotation, so its class has 1 coloring.

Every coloring appears in exactly one class, and indeed

$$1 + 4 + 4 + 2 + 4 + 1 = 16.$$

So there are 6 colorings of the corners of a square up to rotation.

Notice that $16/4 = 4$ is the wrong answer: the classes do not all have 4 elements, because some colorings are unchanged by some rotations. Counting classes of different sizes without listing them is the subject of the next lecture note.

Calling these sets classes makes a claim: the 16 colorings split into sets of colorings that are the same up to rotation, and no coloring lies in two different sets. This claim depends on three properties of the four rotations.

- Every coloring is the same as itself, because the rotation by $0°$ changes nothing.
- If a rotation carries the coloring c to c', then the rotation by the opposite angle carries c' back to c. So "the same up to rotation" does not depend on the order in which the two colorings are named.
- If one rotation carries c to c' and another carries c' to c'', then performing the two rotations in succession is again one of the four rotations, and it carries c to c''.

The third property shows that the class found by repeated rotation of `BBWW` contains every coloring that can be reached from `BBWW`, and the second shows that every member of that class finds the same class. Thus the classes are well defined because the rotations contain the "do nothing" rotation, contain the reverse of each rotation, and are closed under performing one rotation after another. These are the properties that define a group.

13.2 Groups

The rotations of the square rearrange its corners, so we describe them as permutations. A **permutation** of a finite set X is a bijection $X \to X$. For permutations g and h of X, the **composition** gh is the permutation

$$(gh)(x) = g(h(x)),$$

so h is applied first. The **identity** e is defined by $e(x) = x$, and the **inverse** g^{-1} sends $g(x)$ back to x. The rotation of the square by $90°$ counterclockwise is the permutation r of $\{1, 2, 3, 4\}$ with

$$r(1) = 2, \quad r(2) = 3, \quad r(3) = 4, \quad r(4) = 1,$$

since the corner in place i is carried to the place of corner $i+1$, and corner 4 to the place of corner 1. The four rotations are e, r, $r^2 = rr$, and $r^3 = rrr$.

Definition 13.1 (Group). A **group** is a set G together with an operation that assigns to every $g, h \in G$ an element $gh \in G$, such that

1. (associativity) $(gh)k = g(hk)$ for all $g, h, k \in G$;
2. (identity) there is an element $e \in G$ with $eg = ge = g$ for all $g \in G$;
3. (inverses) for every $g \in G$ there is an element $g^{-1} \in G$ with $gg^{-1} = g^{-1}g = e$.

The number of elements $|G|$ is the **order** of G.

The requirement that gh lie in G is the closure property used for the colorings; the identity and inverses are the other two properties. For sets of permutations with composition, associativity holds automatically: $((gh)k)(x)$ and $(g(hk))(x)$ both equal $g(h(k(x)))$. So a set of permutations of X is a group under composition exactly when it contains e, contains the inverse of each of its elements, and contains the composition of any two of its elements.

Example 13.2 (Groups). Each of the following is a group.

- The four rotations $C_4 = \{e, r, r^2, r^3\}$ of the square, with composition. Composing two rotations adds their angles, the identity is e, and the inverse of r is r^3, since turning by 90° and then by 270° is a full turn.
- The set S_n of all permutations of $\{1, \dots, n\}$, with composition. Its order is $n!$. We study it in Section 13.5.
- $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$, where ab is defined as the remainder of $a + b$ on division by n. The identity is 0, and the inverse of $a \neq 0$ is $n - a$.

In $\mathbb{Z}_n$ the operation is addition, written as multiplication only to use one notation for all groups. In $\mathbb{Z}_n$ and in C_4 we always have $ab = ba$, but we will see in Section 13.3 that this fails for the symmetries of the square. The set $\{0, 1, 2, \dots\}$ with addition is not a group, because 1 has no inverse in it.

Powers are defined by $g^0 = e$, $g^m = g \cdots g$ (m factors), and $g^{-m} = (g^{-1})^m$ for $m \geq 1$; then $g^a g^b = g^{a+b}$ for all integers a and b. The following consequences of the axioms hold in every group.

Proposition 13.3 (Basic rules). In a group G:

1. (cancellation) if $gh = gk$ then $h = k$, and if $hg = kg$ then $h = k$;
2. the identity and the inverse of each element are unique;
3. $(gh)^{-1} = h^{-1}g^{-1}$.

Proof. For (1), multiply $gh = gk$ on the left by g^{-1} and use associativity: $h = (g^{-1}g)h = g^{-1}(gh) = g^{-1}(gk) = k$; the second statement is similar. For (2), if e and e' are both identities, then $e = ee' = e'$; if h and k are both inverses of g, then $gh = e = gk$, and cancellation gives $h = k$. For (3), $(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}h = e$, and similarly $(gh)(h^{-1}g^{-1}) = e$. □

Rule (3) reverses the order of the factors: to undo "first h, then g," we first undo g and then undo h.

13.3 The symmetries of a regular polygon

Let $n \geq 3$, and label the corners of a regular n-gon $1, 2, \ldots, n$ counterclockwise. We compute with corner labels modulo n, so that $n+1$ means corner 1 and 0 means corner n. Two corners are **adjacent** if they are joined by a side; the corners adjacent to i are $i-1$ and $i+1$. A rotation or reflection that carries the polygon onto itself preserves distances, so it sends adjacent corners to adjacent corners. We use this as the definition.

Definition 13.4 (Symmetries of a regular polygon). A **symmetry** of the regular n-gon is a permutation g of $\{1, \ldots, n\}$ such that $g(a)$ and $g(b)$ are adjacent whenever a and b are adjacent. The set of symmetries, with composition, is the **dihedral group** D_n.

The set D_n is a group: the composition of two maps that preserve adjacency preserves adjacency, e does, and so does the inverse of a symmetry, because a symmetry sends the n adjacent pairs to n different adjacent pairs, so its inverse sends them back to adjacent pairs.

Where can a symmetry send the corners? The next proposition says that only two pieces of information matter: where corner 1 goes, and whether the images of the corners $1, 2, 3, \ldots$ run counterclockwise or clockwise.

Proposition 13.5 (A symmetry is determined by two choices). Let $g \in D_n$ and $a = g(1)$. Then either $g(i) = a + (i-1)$ for all i, in which case g places the labels counterclockwise, or $g(i) = a - (i-1)$ for all i, in which case g places them clockwise. Conversely, each of these $2n$ maps is a symmetry. In particular, $|D_n| = 2n$.

Proof. Corner 2 is adjacent to corner 1, so $g(2)$ is adjacent to a: either $g(2) = a+1$ or $g(2) = a-1$. Suppose $g(2) = a+1$; we show $g(i) = a + (i-1)$ by induction on i. If $g(i-1) = a + (i-2)$ and $g(i) = a + (i-1)$ for some $2 \leq i < n$, then corner $i+1$ is adjacent to i, so $g(i+1)$ is one of the two neighbors $a + (i-2)$ and $a + i$ of $g(i)$. The first is already $g(i-1)$, and g is one-to-one, so $g(i+1) = a + i$. The case $g(2) = a - 1$ is the same with every sign reversed.
Conversely, for each a the maps $i \mapsto a + (i-1)$ and $i \mapsto a - (i-1)$ are bijections of the corners modulo n, and they send the adjacent corners $i, i+1$ to the adjacent corners $a + (i-1), a + i$ or $a - (i-1), a - i$. There are n choices of a and 2 directions, so $|D_n| = 2n$. □

Every symmetry of the polygon can be built from two particular ones. The **rotation** r turns the polygon by $360^\circ/n$ counterclockwise, so

$$r(i) = i + 1.$$

The **reflection** s flips the polygon across the axis through corner 1 and the center. It fixes corner 1 and exchanges corners that lie symmetrically on the two sides of the axis:

$$s(i) = 2 - i, \qquad \text{that is,} \qquad s(1) = 1,\ s(2) = n,\ s(3) = n-1,\ \ldots.$$

Figure 13.3 shows r and s for the square and for the pentagon. For the square, s fixes corners 1 and 3, which both lie on the axis, and exchanges 2 and 4. For the pentagon, s fixes corner 1 and exchanges 2 with 5 and 3 with 4; the axis passes through corner 1 and the midpoint of the opposite side.

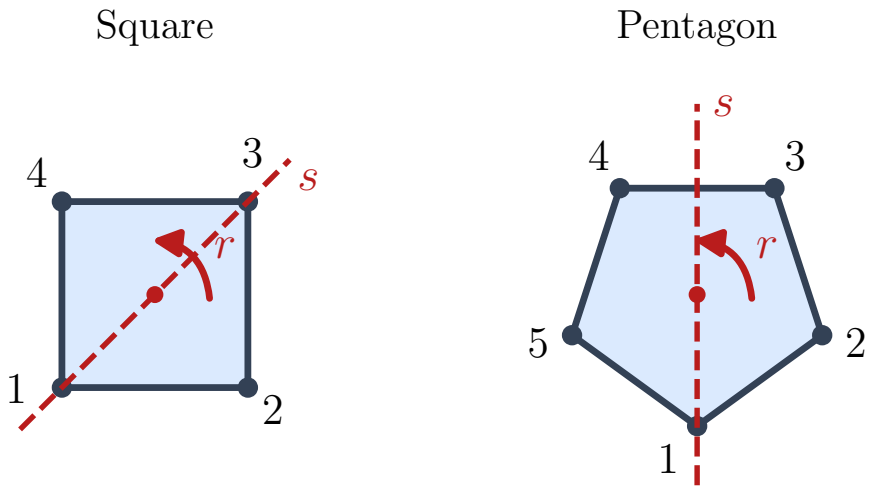

Figure 13.3: The rotation r by $360°/n$ counterclockwise and the axis of the reflection s, which passes through corner 1 and the center, for the square ($n = 4$) and the pentagon ($n = 5$).

Figure description: Left: a square with corners 1 bottom left, 2 bottom right, 3 top right, 4 top left, a counterclockwise arrow labeled r at the center, and a dashed diagonal axis labeled s through corners 1 and 3. Right: a pentagon with corner 1 at the bottom and corners 2 to 5 counterclockwise, the same arrow r, and a dashed vertical axis s through corner 1 and the midpoint of the top side.

To picture a symmetry g, we imagine the labels painted on the corners and move the painted polygon by g: the label i ends up in the place of corner $g(i)$. Figure 13.4 shows the square after the motions e, r, r^2, r^3 in the first row. In each picture the labels still run counterclockwise, and label 1 (in red) has moved one more place. The second row starts from s, where the labels run clockwise, then turns the result by r, and then reflects that result by s. Each new motion is written to the left of the motions already performed, so the second picture is rs, "first s, then r," and the third is srs.

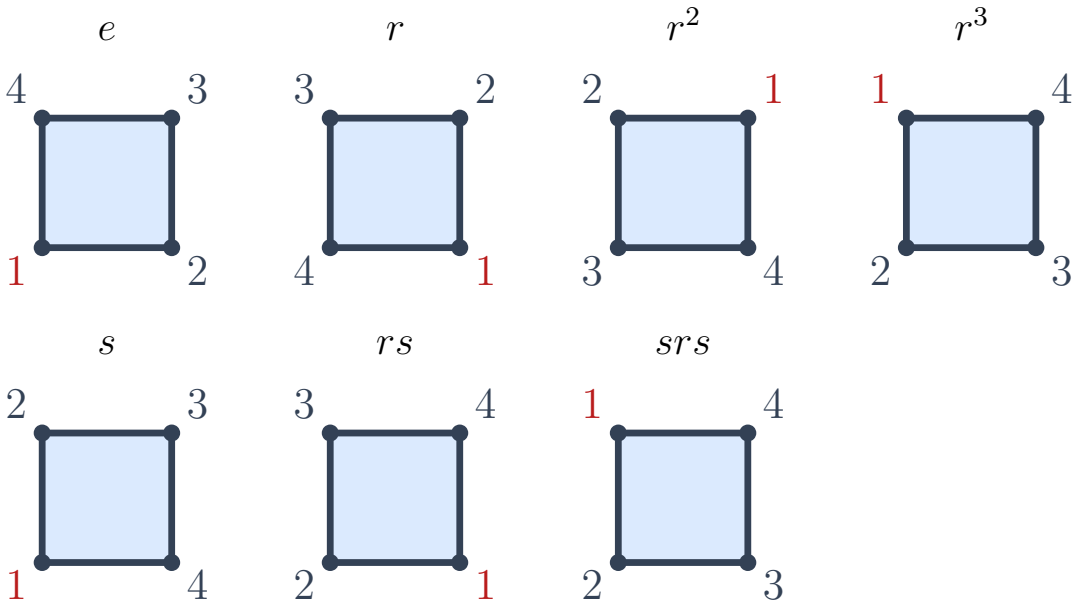

Figure 13.4: The painted square after various motions. In the picture for g, the label i is in the place of corner $g(i)$; label 1 is red. First row: e, r, r^2, r^3. Second row: s, then rs (first s, then r), then srs. The last picture agrees with the picture of r^3.

Figure description: Eight panels arranged in two rows, of which seven show a square with labels at its corners. In the first row the labels run counterclockwise, with label 1 at the bottom left for e, bottom right for r, top right for r squared, and top left for r cubed. In the second row the labels run clockwise for s (1 bottom left, 4 bottom right) and for rs (1 bottom right), and counterclockwise for srs, with label 1 at the top left, as for r cubed.

A permutation of a small set is conveniently written as a table: the top row lists i and the row below lists the image. For the square, each power of r is obtained from the previous one by applying r once more, that is, by adding 1 to every entry of the previous row (with $4+1$ meaning 1):

i	1	2	3	4
$r(i)$	2	3	4	1
$r^2(i)$	3	4	1	2
$r^3(i)$	4	1	2	3
$r^4(i)$	1	2	3	4

The last row is the top row, so $r^4 = e$. For the n-gon, $r^j(i) = i+j$, so $r^n = e$, and the n rotations $e, r, \dots, r^{n-1}$ are different, since r^j sends corner 1 to corner $1+j$. They form the **rotation group** $C_n = \{e, r, \dots, r^{n-1}\}$.

For the square, $s(1) = 1$, $s(2) = 4$, $s(3) = 3$, $s(4) = 2$. Applying s twice returns every corner to its place, so $s^2 = e$; this holds for every n, since $s(s(i)) = 2-(2-i) = i$. To compute srs, we apply s, then r, then s, filling in one row at a time:

i	1	2	3	4
$s(i)$	1	4	3	2
$r(s(i))$	2	1	4	3
$s(r(s(i)))$	4	1	2	3

The last row agrees with the row of r^3 in the previous table, so

$$srs = r^3 = r^{-1}.$$

Figure 13.4 shows the same computation. Geometrically, reflecting, turning counterclockwise, and reflecting back amounts to turning clockwise. The same holds for every n: $srs(i) = s(r(2-i)) = s(3-i) = 2-(3-i) =$

$i - 1 = r^{-1}(i)$. Multiplying $srs = r^{-1}$ on the right by s and using $s^2 = e$ gives the rule

$$sr = r^{-1}s,$$

which tells us how to move s past r. In particular, $rs \neq sr$ for $n \geq 3$, since $rs = sr$ would give $r = r^{-1}$, that is, $r^2 = e$.

The rule $sr = r^{-1}s$ answers the question of which elements make up D_n. The rotation r^j sends corner 1 to $1 + j$ and keeps the counterclockwise order. The product $r^j s$ also sends corner 1 to $1 + j$, since $s(1) = 1$, but it sends corner 2 to $r^j(n) = j$, the corner before $1 + j$; so $r^j s$ places the labels clockwise. By Proposition 13.5, the $2n$ elements

$$r^j s^\varepsilon, \qquad 0 \leq j \leq n - 1, \quad \varepsilon \in \{0, 1\},$$

are exactly the elements of D_n, each listed once. The n elements $r^j s$ are the reflections of the polygon. For the square, the four reflections have the axes shown in Figure 13.5:

$$s = d_{13}, \qquad rs = v, \qquad r^2 s = d_{24}, \qquad r^3 s = h,$$

where v and h are the reflections across the vertical and horizontal axes, and d_{13} and d_{24} are the reflections across the diagonals through corners $1, 3$ and through corners $2, 4$.

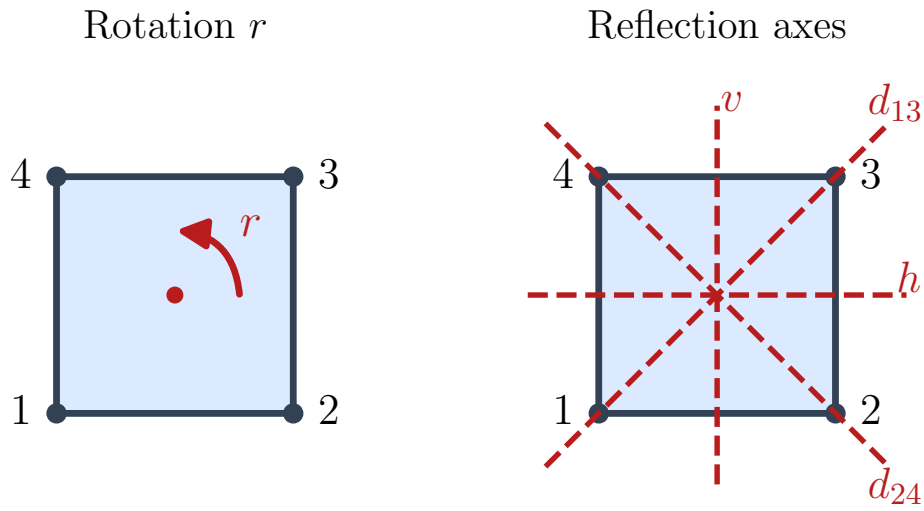

Figure 13.5: The labeled square. Left: the rotation r by 90° counterclockwise. Right: the axes of the reflections v, h, d_{13}, and d_{24}.

Figure description: Two copies of a square with corners labeled 1 bottom left, 2 bottom right, 3 top right, 4 top left. The first shows a counterclockwise arrow labeled r around the center. The second shows four dashed axes: vertical v, horizontal h, the diagonal d13 through corners 1 and 3, and the diagonal d24 through corners 2 and 4.

13.4 Presentations

A table listing all $|G|^2$ products quickly becomes impractical: D_{10} already has 400 products. The previous section suggests a shorter description. A **word** in r and s is a string of these letters, such as $srrsr$, and it stands for the composition of the corresponding symmetries. Every element of D_n is given by some word, and we found three **relations**

$$r^n = e, \qquad s^2 = e, \qquad sr = r^{-1}s.$$

These relations are enough to compute every product. Applying $sr = r^{-1}s$ once for each factor r gives $sr^k = r^{-k}s$, so each s can be moved to the right of each r. Then $s^2 = e$ removes pairs of s's and $r^n = e$

reduces the exponent of r to one of $0, \dots, n-1$. Every word therefore reduces to one of the $2n$ normal forms $r^j s^\varepsilon$.

Example 13.6 (Reducing words). In D_4, $srs = r^{-1}ss = r^{-1} = r^3$, as we found from the tables. In D_5, the word sr^3srs reduces as follows. First $sr^3s = r^{-3}ss = r^{-3}$, so

$$sr^3srs = r^{-3}rs = r^{-2}s = r^3s,$$

using $r^5 = e$ in the last step. The result has the form $r^j s$, so it is a reflection.

We record such a description as a **presentation**, listing the generators and then the relations:

$$D_n = \langle r, s \mid r^n = s^2 = e,\ sr = r^{-1}s \rangle.$$

In the same way $\mathbb{Z}_n = \langle a \mid a^n = e \rangle$ and $C_n = \langle r \mid r^n = e \rangle$.

In general, a presentation $\langle S \mid R \rangle$ describes the group whose elements are words in the generators and their inverses, where two words represent the same element exactly when one can be transformed into the other by inserting or deleting a relation from R, or a pair gg^{-1} or $g^{-1}g$. We do not need the formal construction of this group. A presentation can be finite even when the group is not; for example, $\langle a \mid \rangle$, with no relations, describes the integers under addition. For D_n we could decide when two words are equal because we found normal forms. For a general presentation no such procedure exists.

Theorem (Undecidability for presentations). There is no algorithm that, given a finite presentation and a word in its generators, decides whether the word equals the identity (Novikov 1955, Boone 1958). Consequently, there is no algorithm that, given two finite presentations, decides whether they define the same group; even deciding whether a presentation defines the group with one element is impossible (Adian 1957, Rabin 1958).

These results are proved by building presentations that simulate Turing machines, in the same spirit as the undecidability of the halting problem; the proofs are beyond this course. For a finite group given by explicit permutations, these questions can be decided by checking finitely many cases. This is one reason why, for counting, we work with explicit groups of permutations.

13.5 The symmetric group

The symmetries of a polygon are those permutations of its corners that preserve adjacency. Dropping that condition and allowing every permutation of n objects gives the largest group of permutations of an n-element set.

Definition 13.7 (Symmetric group). The **symmetric group** S_n is the set of all permutations of $\{1, \dots, n\}$, with composition. It has $n!$ elements.

S_n is a group because the composition of two bijections is a bijection, the identity is a bijection, and the inverse of a bijection is a bijection; associativity holds for compositions, as we saw in Section 13.2. The symmetries of the n-gon are some of the elements of S_n, namely those that preserve adjacency. For $n = 3$ every permutation of the corners of a triangle preserves adjacency, so $D_3 = S_3$; for $n \geq 4$, D_n has $2n < n!$ elements.

We write an element of S_n as a table whose top row lists $1, \dots, n$ and whose bottom row lists the images. For example, in S_5 let

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}, \qquad h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}.$$

The identity e is the table whose two rows agree. The inverse g^{-1} reverses every arrow $i \mapsto g(i)$: we exchange the two rows of the table and then sort the columns by the new top row. Since g sends $1 \mapsto 3$, $2 \mapsto 5$, $3 \mapsto 4$, $4 \mapsto 1$, $5 \mapsto 2$, its inverse sends $3 \mapsto 1$, $5 \mapsto 2$, $4 \mapsto 3$, $1 \mapsto 4$, $2 \mapsto 5$:

$$g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

To check, $g(g^{-1}(1)) = g(4) = 1$, and similarly for the other entries.

To compose, we read the tables from right to left. For gh, each x is looked up first in the table of h and then in the table of g: $gh(1) = g(h(1)) = g(2) = 5$, $gh(2) = g(1) = 3$, $gh(3) = g(3) = 4$, $gh(4) = g(5) = 2$, $gh(5) = g(4) = 1$. In the other order, $hg(1) = h(g(1)) = h(3) = 3$. So $gh \neq hg$, and the order of composition matters in S_n as it did in D_n.

A table hides how a permutation moves the elements. Consider

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix} \in S_8.$$

Following 1 through repeated applications of g gives $1 \mapsto 3 \mapsto 6 \mapsto 1$, so these three elements are moved around in a loop. The smallest element not yet visited is 2, and $2 \mapsto 5 \mapsto 2$. Next $g(4) = 4$, so 4 does not move. Finally $7 \mapsto 8 \mapsto 7$. Every element lies on exactly one of the loops $1 \to 3 \to 6 \to 1$, $2 \to 5 \to 2$, $4 \to 4$, $7 \to 8 \to 7$. The next theorem says that this always happens.

Theorem 13.8 (Cycle decomposition). Let g be a permutation of a finite set X and $x \in X$. There is a smallest $l \geq 1$ with $g^l(x) = x$, and the elements $x, g(x), \ldots, g^{l-1}(x)$ are distinct. These elements form the **cycle** of g containing x, written $(x\ g(x)\ \cdots\ g^{l-1}(x))$, and every element of X lies in exactly one cycle.

Proof. The elements $x, g(x), g^2(x), \ldots$ cannot all be different, so $g^i(x) = g^j(x)$ for some $0 \leq i < j$. Applying g^{-1} a total of i times gives $g^{j-i}(x) = x$. Let l be the smallest positive integer with $g^l(x) = x$. If $g^a(x) = g^b(x)$ with $0 \leq a < b < l$, the same argument gives $g^{b-a}(x) = x$ with $0 < b - a < l$, which is impossible; so the listed elements are distinct. Starting from any element of the cycle and applying g runs through the same elements in the same cyclic order, so the cycle containing x is determined by any of its elements, and two cycles that share an element are the same. □

13.6 Cycle notation

Listing the cycles of a permutation describes it completely and shows at once how it moves the elements, so we use the cycles as the standard way to write permutations.

Definition 13.9 (Cycle notation). In **cycle notation** a permutation is written by listing its cycles, each in parentheses: $(a_1\ a_2\ \cdots\ a_l)$ means $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, ..., $a_{l-1} \mapsto a_l$, and $a_l \mapsto a_1$. A cycle with l elements is an **l-cycle**, and a 2-cycle is a **transposition**.

The permutation $g \in S_8$ above is $g = (1\ 3\ 6)(2\ 5)(4)(7\ 8)$. A cycle of length 1 is a **fixed point**: it does not move anything, so cycles of length 1 are usually omitted, and we write $g = (1\ 3\ 6)(2\ 5)(7\ 8)$. Every element not listed is understood to be fixed, and the identity is written e. Because Theorem 13.8 lets a cycle start at any of its elements, $(1\ 3\ 6)$, $(3\ 6\ 1)$, and $(6\ 1\ 3)$ are the same cycle; but $(1\ 6\ 3)$ is a different cycle, sending $1 \mapsto 6$. Reading a cycle backwards gives the inverse: $(a_1\ a_2\ \cdots\ a_l)^{-1} = (a_l\ \cdots\ a_2\ a_1)$.

We write $\mathrm{cyc}(g)$ for the number of cycles of g, *including* the fixed points. The list of the lengths of the cycles, including the fixed points and written in decreasing order, is the **cycle type** of g. The permutation $g \in S_8$

above has $\mathrm{cyc}(g) = 4$ and cycle type $3, 2, 2, 1$. In cycle notation, the eight symmetries of the square are

$$\begin{array}{llll} e, & r = (1\,2\,3\,4), & r^2 = (1\,3)(2\,4), & r^3 = (1\,4\,3\,2), \\ s = d_{13} = (2\,4), & rs = v = (1\,2)(3\,4), & r^2 s = d_{24} = (1\,3), & r^3 s = h = (1\,4)(2\,3). \end{array}$$

So $\mathrm{cyc}(e) = 4$, $\mathrm{cyc}(r) = \mathrm{cyc}(r^3) = 1$, $\mathrm{cyc}(r^2) = \mathrm{cyc}(v) = \mathrm{cyc}(h) = 2$, and $\mathrm{cyc}(d_{13}) = \mathrm{cyc}(d_{24}) = 3$; for instance, d_{13} has the cycles (1), (3), and (2 4). This number will count colorings in the next lecture note: a coloring is unchanged by g exactly when it is constant on each cycle of g.

Each cycle is itself a permutation, which moves the elements of the cycle and fixes all others. Cycle notation such as $(1\,3\,6)(2\,5)(7\,8)$ can therefore also be read as a composition of three permutations. The two readings agree, and the order in which the cycles are written does not matter, because of the following fact. Two cycles are **disjoint** if they have no element in common.

Proposition 13.10 (Disjoint cycles commute). If σ and τ are disjoint cycles, then $\sigma\tau = \tau\sigma$. Consequently, a permutation equals the composition of its cycles, taken in any order.

Proof. Let x be any element. If x lies in σ, then $\sigma(x)$ also lies in σ, so τ fixes both x and $\sigma(x)$. Then $\sigma\tau(x) = \sigma(x)$ and $\tau\sigma(x) = \tau(\sigma(x)) = \sigma(x)$. The case where x lies in τ is the same with the roles exchanged. If x lies in neither cycle, both products fix x. So $\sigma\tau(x) = \tau\sigma(x)$ for every x.
For the second statement, let x lie in the cycle γ of g. In a composition of the cycles of g, every cycle other than γ fixes both x and $\gamma(x) = g(x)$, so the composition sends x to $g(x)$, in any order. □

For example, $(1\,3\,6)(2\,5) = (2\,5)(1\,3\,6)$: in either order, $1 \mapsto 3$, $3 \mapsto 6$, $6 \mapsto 1$, $2 \mapsto 5$, $5 \mapsto 2$, and every other element stays fixed.

When two cycles share an element, Proposition 13.10 does not apply, and the product usually cannot be read off from the factors. The only reliable method is to follow each element through the factors from right to left. Let us compute $g = (1\,2\,4\,5)(3\,4)$ in S_5, applying $(3\,4)$ first:

$$1 \mapsto 1 \mapsto 2, \qquad 2 \mapsto 2 \mapsto 4, \qquad 3 \mapsto 4 \mapsto 5, \qquad 4 \mapsto 3 \mapsto 3, \qquad 5 \mapsto 5 \mapsto 1.$$

Following g from 1 gives $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 5 \mapsto 1$, so

$$(1\,2\,4\,5)(3\,4) = (1\,2\,4\,3\,5).$$

In the other order we apply $(1\,2\,4\,5)$ first:

$$1 \mapsto 2 \mapsto 2, \qquad 2 \mapsto 4 \mapsto 3, \qquad 3 \mapsto 3 \mapsto 4, \qquad 4 \mapsto 5 \mapsto 5, \qquad 5 \mapsto 1 \mapsto 1,$$

so

$$(3\,4)(1\,2\,4\,5) = (1\,2\,3\,4\,5).$$

The two products are different: one sends $2 \mapsto 4$ and the other $2 \mapsto 3$. Both are 5-cycles, although the factors are a 4-cycle and a transposition, so even the cycle type of a product cannot be read from the cycle types of overlapping factors. A common error is to apply the left factor first; in this example that error turns one answer into the other.

13.7 Conjugation

Sometimes two permutations do the same thing to differently named elements. In the square, $d_{13} = (2\,4)$ and $d_{24} = (1\,3)$ are both reflections across a diagonal, and turning the square by r carries the first diagonal to the second. Conjugation makes this kind of renaming precise.

Definition 13.11 (Conjugate). Let g and σ be elements of a group G. The **conjugate** of σ by g is $g\sigma g^{-1}$.

For permutations, $g\sigma g^{-1}$ first undoes g, then applies σ, then applies g again. If we think of g as renaming each element x as $g(x)$, then $g\sigma g^{-1}$ does to the new names what σ did to the old ones.

Proposition 13.12 (Conjugation relabels cycles). Let $g, \sigma \in S_n$. If $\sigma(a) = b$, then $g\sigma g^{-1}$ sends $g(a)$ to $g(b)$. Consequently, the cycle notation of $g\sigma g^{-1}$ is obtained from that of σ by replacing every entry x by $g(x)$:

$$g\,(a_1\ a_2\ \cdots\ a_l)\,g^{-1} = (g(a_1)\ g(a_2)\ \cdots\ g(a_l)),$$

and similarly for each cycle of σ. In particular, σ and $g\sigma g^{-1}$ have the same cycle type.

Proof. We compute $g\sigma g^{-1}(g(a)) = g(\sigma(g^{-1}(g(a)))) = g(\sigma(a)) = g(b)$. Each arrow $a \mapsto b$ of σ therefore becomes the arrow $g(a) \mapsto g(b)$ of $g\sigma g^{-1}$. Since g is a bijection, every element has the form $g(a)$, so these arrows describe $g\sigma g^{-1}$ completely. A cycle $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_l \mapsto a_1$ of σ becomes the cycle $g(a_1) \mapsto \cdots \mapsto g(a_l) \mapsto g(a_1)$ of the same length. □

Example 13.13 (Conjugates in the square). With $r = (1\ 2\ 3\ 4)$ and $s = (2\ 4)$, the proposition gives

$$rsr^{-1} = (r(2)\ r(4)) = (3\ 1) = d_{24}.$$

Turning the square by 90° carries the axis of s, through corners 1 and 3, to the diagonal through corners 2 and 4, and the conjugate is the reflection across that rotated axis. In the other direction, since $s^{-1} = s$,

$$srs^{-1} = srs = (s(1)\ s(2)\ s(3)\ s(4)) = (1\ 4\ 3\ 2) = r^3,$$

which recovers $srs = r^{-1}$ without a table: the conjugate of a rotation by a reflection is the rotation in the opposite direction.

Example 13.14 (Conjugates in S_5). Let $\sigma = (1\ 2\ 3)(4\ 5)$ and $g = (1\ 4)(2\ 5)$, so that $g(1) = 4$, $g(2) = 5$, $g(3) = 3$, $g(4) = 1$, $g(5) = 2$. Replacing each entry of σ by its image under g gives

$$g\sigma g^{-1} = (4\ 5\ 3)(1\ 2).$$

As a check, $g^{-1} = g$, and $g\sigma g^{-1}(1) = g(\sigma(g(1))) = g(\sigma(4)) = g(5) = 2$, in agreement with the transposition $(1\ 2)$. Both σ and its conjugate have cycle type $3, 2$.

The converse of the last statement in Proposition 13.12 also holds in S_n: if σ and τ have the same cycle type, write both in cycle notation including fixed points, with cycles of equal length in the same positions, and let g send each entry of σ to the entry of τ in the same position. Then $g\sigma g^{-1} = \tau$. So two permutations in S_n are conjugate exactly when they have the same cycle type.

13.8 Subgroups and the order of an element

The rotations C_n form a group sitting inside D_n, and D_n is a group sitting inside S_n. Such smaller groups have a name.

Definition 13.15 (Subgroup). A **subgroup** of G is a subset $H \subseteq G$ that is a group with the same operation: $e \in H$, and $gh \in H$ and $g^{-1} \in H$ whenever $g, h \in H$. A subgroup of the group of all permutations of a set X is a **permutation group** on X.

The rotations $C_4 = \{e, r, r^2, r^3\}$ form a subgroup of D_4, and so does $\{e, s\}$, since $s^2 = e$. The set $\{0, 2\}$ is a subgroup of $\mathbb{Z}_4$. The permutations in S_n that fix n form a subgroup with $(n-1)!$ elements. The groups D_n and C_n are permutation groups on the corners of the n-gon. For finite subsets, closure under the operation is the only condition that needs checking.

Proposition 13.16 (Subgroup test for finite sets). Let G be a group and H a finite nonempty subset with $gh \in H$ whenever $g, h \in H$. Then H is a subgroup.

Proof. Let $g \in H$. By closure, $g, g^2, g^3, \ldots$ all lie in H. Since H is finite, $g^i = g^j$ for some $1 \leq i < j$, and cancelling g^i gives $g^{j-i} = e$. So $e \in H$, and $g^{-1} = g^{j-i-1}$ (which is e if $j - i = 1$) also lies in H. □

The proof shows that some power of every element g of a finite group equals e. The first such power measures how many times g must be repeated before everything returns to its starting place.

Definition 13.17 (Order of an element). The **order** of an element g of a finite group is the smallest positive integer m with $g^m = e$.

Such an m exists by the argument in Proposition 13.16. In D_4, the rotations r and r^3 have order 4, the five other elements besides e have order 2, and e has order 1. In $\mathbb{Z}_6$, the element 2 has order 3, since $2+2+2 = 6$ is the first multiple of 2 divisible by 6.

Proposition 13.18 (Powers and order). Let g have order m. Then $g^k = e$ exactly when m divides k, and $e, g, \ldots, g^{m-1}$ are distinct. For a permutation, the order is the least common multiple of its cycle lengths.

Proof. Write $k = qm + t$ with $0 \leq t < m$. Then $g^k = (g^m)^q g^t = g^t$, which equals e exactly when $t = 0$, by the minimality of m. If $g^a = g^b$ with $0 \leq a < b < m$, cancellation gives $g^{b-a} = e$ with $0 < b - a < m$, which is impossible. For a permutation g, an element on a cycle of length l returns to itself after k steps exactly when l divides k, so $g^k = e$ exactly when k is a common multiple of the cycle lengths; the smallest such k is their least common multiple. □

For example, $(1\ 2)(3\ 4\ 5) \in S_5$ has order $\operatorname{lcm}(2, 3) = 6$. Every order we have found so far divides the order of the group: orders 1, 2, 4 in D_4, and 3 in $\mathbb{Z}_6$. This always happens.

Theorem 13.19 (The order of an element divides the order of the group). Let G be a finite group and $g \in G$. Then the order of g divides $|G|$, and $g^{|G|} = e$.

Proof. Let m be the order of g. Multiplication on the right by g, the function $\rho(x) = xg$, is a permutation of G; it is undone by $x \mapsto xg^{-1}$. By Theorem 13.8, G splits into the cycles of ρ. The cycle of ρ containing x has length equal to the smallest $l \geq 1$ with $\rho^l(x) = x$, that is, $xg^l = x$. By cancellation, $xg^l = x$ exactly when $g^l = e$, so every cycle has length exactly m. The $|G|$ elements of G are therefore split into cycles of m elements each, so m divides $|G|$, and $g^{|G|} = e$ by Proposition 13.18. □

For instance, no symmetry of the square has order 3, since 3 does not divide 8. If $|G| = p$ is prime, every element other than e has order p, so its p powers are all of G.

The divisibility goes in one direction only: 6 divides $|S_4| = 24$, but the cycle types of elements of S_4 are $1, 1, 1, 1$; $2, 1, 1$; $2, 2$; $3, 1$; and 4, so their orders are 1, 2, 3, 4, and no element of S_4 has order 6.

Theorem 13.19 is a special case of a statement about subgroups. If g has order m, then the powers $e, g, \ldots, g^{m-1}$ form a subgroup with m elements, as we show in Section 13.9, so the theorem says that the order of this subgroup divides $|G|$.

Theorem 13.20 (Lagrange's theorem). If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

We prove Lagrange's theorem in the next lecture note, where it follows from the orbit–stabilizer theorem in the same way that Theorem 13.19 followed from the cycles of ρ. For example, every subgroup of D_4 has order 1, 2, 4, or 8, so no three symmetries of the square form a group.

13.9 Cyclic groups

The rotation group C_n consists of the powers of the single rotation r, and every element of $\mathbb{Z}_n$ is obtained by adding 1 to itself repeatedly. Groups built from one element in this way are the simplest groups, and the number of elements they contain turns out to be the order of that element.

Definition 13.21 (Cyclic subgroup). Let g be an element of a finite group G. The **cyclic subgroup generated by** g is the set

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

of all powers of g, with positive, zero, and negative exponents.

The definition lists infinitely many powers, but in a finite group only finitely many of them are different, and the order of g tells us exactly how many.

Proposition 13.22 (Order of an element and size of its cyclic subgroup). Let $g \in G$ have order m. Then

$$\langle g \rangle = \{e, g, g^2, \dots, g^{m-1}\},$$

these m powers are distinct, and $\langle g \rangle$ is a subgroup of G. In particular, $|\langle g \rangle|$ equals the order of g.

Proof. Let k be any integer, and divide by m with remainder: $k = qm + t$ with $0 \le t < m$. This works for negative k as well; for example, $-1 = (-1)m + (m-1)$. Since m divides qm, Proposition 13.18 gives $g^{qm} = e$, so $g^k = g^{qm}g^t = g^t$. Thus every power of g is one of $e, g, \dots, g^{m-1}$, and these are distinct by Proposition 13.18.
The set $\langle g \rangle$ contains $e = g^0$. The product $g^a g^b = g^{a+b}$ of two powers of g is a power of g, and so is the inverse g^{-a} of g^a. So $\langle g \rangle$ is a subgroup. □

Example 13.23 (Cyclic subgroups). In D_4, the powers of r are e, r, r^2, r^3, so $\langle r \rangle = C_4$ has 4 elements, matching the order 4 of r. The reflection s has order 2, and $\langle s \rangle = \{e, s\}$.
In $\mathbb{Z}_6$, the powers of a are the remainders of $0, a, 2a, 3a, \dots$ on division by 6. So $\langle 2 \rangle = \{0, 2, 4\}$ and $\langle 3 \rangle = \{0, 3\}$, with 3 and 2 elements, the orders of 2 and 3. The multiples of 5 give the remainders $0, 5, 4, 3, 2, 1$, so $\langle 5 \rangle = \langle 1 \rangle = \mathbb{Z}_6$. Different elements can generate the same cyclic subgroup.

Proposition 13.22 turns Theorem 13.19 into a statement about subgroups: the order of g is the number of elements of the subgroup $\langle g \rangle$, so once Lagrange's theorem is proved, it gives a second proof that the order of g divides $|G|$.

Definition 13.24 (Cyclic group). A group G is **cyclic** if $G = \langle g \rangle$ for some $g \in G$. Such an element g is called a **generator** of G.

Since $\langle g \rangle$ has as many elements as the order of g, and $\langle g \rangle \subseteq G$, a finite group G equals $\langle g \rangle$ exactly when g has order $|G|$. So a finite group is cyclic exactly when it contains an element whose order equals the order of the group, and its generators are exactly the elements of that order.

Example 13.25 (Cyclic and non-cyclic groups). The rotation group $C_n = \langle r \rangle$ is cyclic, and so is $\mathbb{Z}_n = \langle 1 \rangle$. By Example 13.23, the generators of $\mathbb{Z}_6$ are 1 and 5; the elements 0, 2, 3, and 4 have orders 1, 3, 2, and 3, smaller than 6.
The group D_4 has 8 elements, but its elements have orders 1, 2, and 4, so D_4 is not cyclic. There is also a reason that applies to every $n \geq 3$. In a cyclic group, any two elements g^a and g^b commute, since $g^a g^b = g^{a+b} = g^b g^a$. In D_n with $n \geq 3$ we found $rs \neq sr$, so D_n is not cyclic. For the same reason S_3 is not cyclic: following each element from right to left gives $(1\ 2)(1\ 3) = (1\ 3\ 2)$ but $(1\ 3)(1\ 2) = (1\ 2\ 3)$.

A group in which all elements commute need not be cyclic. The subgroup $\{e, r^2, v, h\}$ of D_4, consisting of the symmetries of the square that also carry a non-square rectangle onto itself, is a subgroup. Using $v = rs$, $h = r^3 s$, and $(r^j s)(r^k s) = r^{j-k}$, we find $vh = hv = r^2$, and $r^2 v = h$, $r^2 h = v$; moreover r^2 commutes with every element of D_4, because $sr^2 = r^{-2}s = r^2 s$. So any two elements of this subgroup commute, but every element has order 1 or 2, and none has order 4; the subgroup is not cyclic.

The group $\mathbb{Z}_4$ is defined by addition, not by permutations, but it behaves exactly like the rotation group C_4: matching j with r^j, adding residues corresponds to composing rotations. Two groups that match in this way are considered the same.

Definition 13.26 (Isomorphism). An **isomorphism** from a group G to a group K is a bijection $\varphi\colon G \to K$ with $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$. If one exists, G and K are **isomorphic**.

The match between $\mathbb{Z}_4$ and C_4 is an instance of a general fact: a cyclic group is determined, up to the names of its elements, by its order.

Proposition 13.27 (Cyclic groups of order m). If $G = \langle g \rangle$ is a cyclic group with m elements, then $\varphi(j) = g^j$ defines an isomorphism $\varphi\colon \mathbb{Z}_m \to G$.

Proof. By Proposition 13.22, g has order m and the powers $g^0, g^1, \ldots, g^{m-1}$ are the m distinct elements of G, so φ is a bijection. For $j, k \in \mathbb{Z}_m$, the product jk in $\mathbb{Z}_m$ is the remainder t of $j + k$ on division by m. As in the proof of Proposition 13.22, $g^{j+k} = g^t$, since m divides $j + k - t$. Therefore $\varphi(jk) = g^t = g^{j+k} = g^j g^k = \varphi(j)\varphi(k)$. □

For example, the rotation group C_n is isomorphic to $\mathbb{Z}_n$, and the subgroup $\{e, s\}$ of D_4 is isomorphic to $\mathbb{Z}_2$. A group of prime order p is cyclic: by Theorem 13.19, an element $g \neq e$ has an order that divides p and is not 1, so it has order p and $\langle g \rangle = G$. By Proposition 13.27, every group of prime order p is isomorphic to $\mathbb{Z}_p$.

13.10 Cayley's theorem

Every finite group is isomorphic to a permutation group. The permutations come from the group itself: each element g rearranges the elements of G by multiplication on the left.

Theorem 13.28 (Cayley's theorem). Let G be a finite group. For $g \in G$, define $\lambda_g\colon G \to G$ by $\lambda_g(x) = gx$. Then each λ_g is a permutation of G, the set $\Lambda = \{\lambda_g : g \in G\}$ is a permutation group on G, and $g \mapsto \lambda_g$ is an isomorphism from G to Λ. In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof. Step 1: Each λ_g is a permutation.
By associativity, $\lambda_{g^{-1}}(\lambda_g(x)) = g^{-1}(gx) = (g^{-1}g)x = x$, and similarly $\lambda_g(\lambda_{g^{-1}}(x)) = x$. So $\lambda_{g^{-1}}$ undoes λ_g, and λ_g is a bijection.

Step 2: Products correspond to compositions.
For all x, $\lambda_{gh}(x) = (gh)x = g(hx) = \lambda_g(\lambda_h(x))$, so $\lambda_{gh} = \lambda_g\lambda_h$.

Step 3: Different elements give different permutations.
$\lambda_g(e) = g$, so $\lambda_g = \lambda_h$ implies $g = h$.

Step 4: Conclusion.
By Step 2, Λ is closed under composition, so by Proposition 13.16 it is a permutation group on G. By Steps 2 and 3, $g \mapsto \lambda_g$ is a bijection from G to Λ that turns products into compositions, that is, an isomorphism. Numbering the elements of G as $1, \dots, n$ turns permutations of G into elements of S_n. □

Example 13.29 (Cayley's theorem for $\mathbb{Z}_4$). In $\mathbb{Z}_4$, the element 1 gives $\lambda_1(x) = x + 1$, which sends $0 \mapsto 1 \mapsto 2 \mapsto 3 \mapsto 0$; so $\lambda_1 = (0\ 1\ 2\ 3)$. Similarly $\lambda_2 = (0\ 2)(1\ 3)$ and $\lambda_3 = (0\ 3\ 2\ 1)$. Up to the names of the four elements, these are the rotations r, r^2, r^3 of the square.

Cayley's theorem means that studying permutation groups loses no finite groups. In the rest of this unit every group will be given as a group of permutations.

Problem (Check yourself). Sort the $2^3 = 8$ black-and-white colorings of the corners of an equilateral triangle into classes up to rotation. Using the relations of D_4, write rsr^2s in the form $r^j s^\varepsilon$, and check the answer with tables. Compute $(1\ 3\ 5)(1\ 2)$ and $(1\ 2)(1\ 3\ 5)$ in S_5, and find the conjugate of $(1\ 2\ 3\ 4)$ by $(1\ 3)$. Find the order of $(1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9) \in S_9$. List the elements of $\langle 3 \rangle$ and $\langle 6 \rangle$ in $\mathbb{Z}_8$, find all generators of $\mathbb{Z}_8$, and decide whether D_3 is cyclic.