Computations in Groups

We consider a general group G, not necessarily infinite, and write the group operation multiplicatively. It is a good exercise to translate our results below into additive notation. Typically, + is used for abelian groups.

1. For any subsets A, B, etc. (not necessarily subgroups) of G, we define

   $$AB :=$$

   $$A^{-1} :=$$

   One or both sets could be singletons, like $\{g\}$, with $g \in G$. Then it is nicer to write Ag instead of $A\{g\}$, etc.

   We thus treat such sets as individual entities. This is a very useful way to think and is at the heart of 'quotienting' in algebra and geometry.

2. Prove

   - $(AB)C = A(BC)$

   - $(AB)^{-1} =$ (what?)

   - $(A^{-1})^{-1} =$ (what?)

3. Suppose now that H is a subgroup of G, written $H \leqslant G$. For any $g \in H$ we say that the subset Hg is a *right coset* of H and that gH is a *left coset* of H. For left-to-right computations, right cosets are typically more convenient. Many of the claims below will have obvious left-hand variants.

   Prove for elements x, g, etc. of G and the subgroup H:

   - $HH = H$

   - $H^{-1} = H$

   - $g \in H \Longleftrightarrow Hg = gH = H$

   - $x \in Hg \Longleftrightarrow Hg = Hx$

     Remark: any element of this coset, in particular either of x or g, is considered to be a (right) *coset representative* for the coset.

   - $Hg_1 \cap Hg_2 \neq \emptyset \Rightarrow Hg_1 = Hg_2$.

   - Each element $x \in G$ belongs to exactly one coset of a given subgroup H.

- Any two cosets have the same cardinality, since there is a bijection

  $$Hg_1 \to Hg_2$$

  defined by ...

4. **Definition** If $H \leqslant G$, the *index* of H in G, written $[G : H]$, is the number of (right) cosets of H in G.

   (Prove that this equals the number of left cosets, too.)

5. Prove *Lagrange's Theorem*: If G is finite and $H \leqslant G$, then $|H|$ divides $|G|$ and

   $$[G : H] = \frac{|G|}{|H|}$$

   Remark. One can make sense of this when G is infinite, too.

6. **Definition**: Suppose H is a subgroup of G. Then a (right) *transversal* T for H in G is a set of coset representatives, *exactly one for each coset* of H.

   Remarks: Thus the intersection $T \cap Hx$ always has size one. However, the element in this singleton set might not be x. Yes, it will be x if by chance x was the representative in T chosen for the coset Hx.

   Notice that $1 \in H$, so that 1 does represent $H = H1$ itself. Typically we (and Gap, too) make this standard choice for the representative of the subgroup. If we follow this convention then
$$T \cap H = \{1\}$$

   Also note that the cardinality of T is just the number of cosets, since we chose one representative for each coset. Thus $|T| = [G : H]$, the index. So T is finite if G itself is finite, but also in other cases.

7. **Definition**. Fix a (standard) transversal T for the subgroup H in G. Then we may define a 'transversal function'
$$\begin{array}{ccc} G & \longrightarrow & T \\ x & \longmapsto & \overline{x} \end{array}$$

   where $\overline{x}$ is the representative (in T) for the coset Hx.

   For example, given our standard choice of 1 for H itself, we have $\overline{x} = 1$ if and only if $x \in H$. (Prove this for yourself.)

8. Prove these properties of the bar function for $x, y \in G$ and $t \in T$:

   - $\overline{\overline{x}} = \overline{x}$

- $\overline{x}\,x^{-1} \in H$

- $\overline{xy} = \overline{\overline{x}y}$

- $\overline{\overline{tx}\,x^{-1}} = t$

9. Prove that if the right coset Hg equals some left coset, then $Hg = gH$, or equivalently, $g^{-1}Hg = H$.

   Remark: We could say g commutes with H (in bulk, possibly not with the individual members of H).

10. **Definition** (one of many equivalent versions). The subgroup H of G is *normal*, written $H \triangleleft G$, if every right coset of H is also a left coset.

    Remark. This amounts to the more useful criterion that $g^{-1}Hg \subseteq H$ for all $g \in G$.

11. If $H \triangleleft G$ prove that

$$Hg_1Hg_2 = H(g_1g_2)$$

for all $g_1, g_2 \in G$.

12. **Remark and Definition**

    This means that coset multiplication is a closed operation. It follows at once that the set G/H of all cosets becomes a group with this operation. This is the *quotient group*.

    The identity in G/H is H; and $(Hg)^{-1} = H(g^{-1})$. (Check these claims!)

    Each coset Hg is treated as an individual entity; in effect, this blurs the distinction between individual elements of the coset. In other words, elements a, b of G are identified when they belong to the same coset, namely when $ab^{-1} \in H$.

13. Suppose $\{H_j : j \in \mathcal{J}\}$ is any collection of subgroups of a given group G. (The index set can be finite or not; the individual groups can be finite or not.) Show that

    $$H = \bigcap_{j \in \mathcal{J}} H_t$$

    is a subgroup of G.

    Remark. Thus any intersection of subgroups is a subgroup. In particualar, if H_1 and H_2 are subgroups of G then so is $H_1 \cap H_2$.

14. **Definition**. Let X be any subset of the group G. X need not be a subgroup. By a *word* in X we mean any product

    $$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k}$$

    where $\varepsilon_j = \pm 1$ and each $x_j \in X$. For example,

    $$1 = x_1^1 \cdot x_1^{-1}$$
    $$x_1^3 = x_1^1 x_1^1 x_1^1$$
    $$x_1 x_2^{-1} x_1 x_3 x_4^{-1}$$

    are all words in $X = \{x_1, x_2, x_3, x_4\}$.

The subgroup *generated* by X is the set of all words in X. We write

$$\langle X \rangle = \{\text{words } \ x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k} \ \text{ in } \ X\}.$$

15. Verify that $\langle X \rangle$ is indeed a subgroup of G.

16. Show that $\langle X \rangle$ is the intersection of <u>all</u> subgroups of G which contain X. (There is at least one such subgroup, namely G itself.)

    Remark: this provides an alternative definition for the subgroup generated by a subset X of the group G. Intuitively, we may therefore say that $\langle X \rangle$ is the *smallest* subgroup which contains the set X.

17. Suppose now that X is a set of generators for group G, so that $G = \langle X \rangle$. Let H be a subgroup and let T be a fixed transversal T for H in G.

    We will use the bar function $\overline{} : G \to T$ to manufacture a set of generators for the subgroup H. This algorithm (due to Schreier) is important (in Gap, for example). I am copying the treatment in Larry Groves's *Groups and Characters*.

    We let $X^{\pm} = X \cup X^{-1}$ and define two subsets of G as follows:

$$\begin{aligned} A &:= \{tx(\overline{tx})^{-1} \,:\, t \in T \text{ and } x \in X^{\pm}\} \\ B &:= \{tx(\overline{tx})^{-1} \,:\, t \in T \text{ and } x \in X\} \end{aligned}$$

    Thus B is merely a subset of A, since we just restrict the possibilities for x (generators only for B; also their inverses, if it makes any difference, for A).

18. Prove that $B \subseteq A \subseteq H$.

19. Prove that $A \subseteq B \cup B^{-1} \cup \{1\}$.

20. Prove that the $\langle A \rangle = \langle B \rangle$ (i.e. equal subgroups with possibly different sets of generators).

21. **Schreier's Theorem** The subgroup H is generated by the set $B = \{tx(\overline{tx})^{-1} \,:\, t \in T \text{ and } x \in X\}$ (from above).

Symmetric Groups

1. Let X be any set. A bijection from a set X to itself is often called a *permutation* on X; another synonym is *rearrangement.*

   The collection of all such bijections, with left-to-right composition of functions, is the *symmetric group* $\mathbb{S}_X$.

   If $x \in X$ and $f, g \in \mathbb{S}_X$, then it seems we should write $(x)f$, instead of $f(x)$; and composition becomes $((x)f)g$ (meaning first apply f then g).

   But this is awkward, so we often use the 'exponential' alternative

   $$x^f$$

   (in place of $f(x)$). Then composition is defined by the very natural looking rule

   $$x^{fg} := (x^f)^g \ .$$

   Indeed, this is so in Gap, where exponentiation is indicated by the caret ˆ :

   ```
   gap> # Here is a permutation in S_6:
   gap> f:= (1,4,5,2)(3,6);
   (1,4,5,2)(3,6)
   gap> # Here are some elements in the ground set [1..6]
   gap> x:=4;y:=6;
   4
   6
   gap> x^f; y^f;
   5
   3
   ```

2. The actual nature of the elements of the *ground set* X is often immaterial. When X has finite cardinality, say

   $$|X| = n \ ,$$

   it is convenient to take

   $$X = \{1, \ldots, n\},$$

   in which case we often write $\mathbb{S}_n$ in place of $\mathbb{S}_X$.

Notation. $\mathbb{S}_n$ is the symmetric group of permutations on $\{1, \ldots, n\}$. Note that $\mathbb{S}_n$ has order $n!$.

Remarks. Such groups are well suited to computer implementation; there are many efficient algorithms for computing with permutations.

The shorthand $[n] := \{1, \ldots, n\}$ is frequently used in algebra and combinatorics. Thus a permutation is a bijection

$$f : [n] \to [n] \; .$$

3. **Visualizing general functions $f : [n] \to [n]$ (including bijections)**

We can use graphs, arrow digrams or cycle notation. The latter device is efficient and is precisely how we represent permutations in a computer language like GAP. The case $n = 4$ is typical enough, so we will take

$$X = [4] = \{1, 2, 3, 4\} \; .$$

(a) Here are some functions represented as conventional graphs in $\mathbb{R}^2$:

Actually, each graph is embedded in the grid

$$[4]^2 = [4] \times [4] = \{1, 2, 3, 4\} \times \{1, 2, 3, 4\} \; .$$

Note that f is not onto hence also not 1–1. Thus $f \notin \mathbb{S}_4$. However, g and h are typical permutations in $\mathbb{S}_4$.

Since the graph lives in the 4×4 grid, it makes no sense to join up the dots by line segments! We begin to see that the positions of 1,2,3,4 on the axes are irrelevant. As a matter of fact, the symbols themselves are somewhat arbitrary. We could just as well permute four other symbols, like

$$\alpha, \beta, \gamma, \delta$$

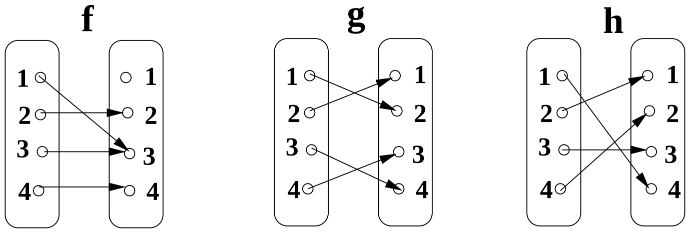
or

$$\heartsuit, \diamondsuit, \clubsuit, \spadesuit \; ,$$

which have no natural positions in a graph. The mathematical content of the permutations would be unaltered by such a change in the ground set.

However, we stick with 1,2,3,4, since these symbols are familiar and are easy to enter into the computer.

(b) The same three functions are more naturally represented by these arrow diagrams:



Note how easy it is to pick out the 1–1 or onto functions. In fact, we easily see why 1–1 is equivalent to onto for *finite* ground sets X.

(c) Now we investigate cycle notation, which is appropriate only for bijections. Let's look at the function h, which could be fully described by the following cumbersome setup:

$$\begin{aligned} 1h &= 4 \\ 2h &= 1 \\ 3h &= 3 \\ 4h &= 2 \end{aligned}$$

The fact that we see a rearrangement of 1,2,3,4 in the right-hand column confirms that h is a bijection. Here is a slightly more compact way of representing the same information:

$$1 \xrightarrow{h} 4 \xrightarrow{h} 2 \xrightarrow{h} 1 \text{ and } 3 \xrightarrow{h} 3\ .$$

The cycle representation for H is just an abbreviation of this. Here is how it works.

Start with any element of the ground set, say $x = 1$ to be specific, and track where that element is sent by h (here 4), then where that 4 is sent by h (here to 2), and so forth. You will find that your list of elements closes up into a so-called *cycle*. For example, h sends 2 back to the initial element 1. This information can be compressed as follows:

$$(1, 4, 2)\ .$$

Note that we scan a cycle left to right and that each element is mapped by h to the one just after, except that the right-most element is mapped to the front element of the cycle.

Now repeat the process for any unaccounted-for elements in the ground set and manufacture more such cycles.

To finish off our h we note that the remaining element 3 must belong to a trivial cycle (3), indicating that 3 is a *fixed point* for h. When done we may express h as a product of *disjoint* cycles, namely

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

Note that the same information is conveyed if we start any particular cycle at another of its elements. Thus

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

If the context is clear, that is to say, if we know we are permuting $\{1, 2, 3, 4\}$, then trivial cycles are often suppressed and understood. In fact, GAP will do just that and print h as

$$(1, 4, 2) \ .$$

Clearly, the above process works for any bijection on a finite set. One encodes the mapping information in a collection of disjoint (i.e. non-overlapping) cycles.

(d) **The identity permutation and inverses**

The notation 1 for the identity function would now be a bit confusing; so let us use e to denote the identity permutation on [4]. Thus e fixes every element and so

$$e = (1)(2)(3)(4) .$$

After suppressing trivial cycles, GAP would write $e = ()$.

It is easy to write the inverse of a permutation given in cycle form. Since the inverse merely reverses all arrows in an arrow diagram, we must rewrite each of the disjoint cycles in reverse order. Again the starting element for each cycle is a matter of choice. For example,

$$h^{-1} = (1, 2, 4)(3) .$$

Trivial cycles, in fact also cycles of length 2, are unaffected by switching to the inverse.

As another example, consider g from above. We can convey the mapping information for g in several ways, so it is quite legal to write

$$g = (1, 2)(3, 4) = (3, 4)(1, 2) = (2, 1)(3, 4) .$$

Since every cycle has length 2, g must be self-inverse: $g = g^{-1}$, just like a reflection.

(e) **Products**

Multiplying permutations in cycle format is is easy – just remember to scan left to right. For example, g maps 1 to 2 and h maps 2 to 1, so gh maps 1 to 1. Now move on to input 2: g maps 2 to 1 and h maps 1 to 4, so gh maps 2 to 4. Next move to input 4 and continue. With practice one can write out products without any effort:

$$gh = (1, 2)(3, 4) \cdot (1, 4, 2)(3) = (1)(2, 4, 3) = (2, 4, 3)$$

and

$$hg = (1, 4, 2)(3) \cdot (1, 2)(3, 4) = (1, 3, 4)(2) = (1, 3, 4) .$$

Notice that we end up with disjoint cycles, even though at intermediate steps we might not have disjoint cycles. Also note here that $gh \neq hg$.

(f) **Theorem**. Every permutation $f \in \mathbb{S}_n$ can be factored as a product of disjoint cycles an essentially unique way.

Proof. See any text on group theory. The argument just tightens up our informal discussion above. □

Even and odd permutations

1. An m-cycle in $\mathbb{S}_n$ is a permutation which can be written as a single cycle, say

$$c = (a_1, \dots, a_m) \ ,$$

where $a_1, \dots, a_m$ are distinct elements taken from $\{1, \dots, n\}$ in any particular order. Of course, this means $m \leqslant n$; and again we have suppressed fixed points (i.e. 1-cycles).

A 2-cycle $t = (a, b)$ is often called a *transposition*.

2. We have seen that we can factor a general permutation as a product of disjoint cycles.

We now observe that any individual cycle can be factored as a product of transpositions, typically in several different ways. These transpositions are unlikely to be disjoint, however. Our proof is by construction:

$$(a_1, \dots, a_m) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_m) \ .$$

For example,

- $(1,3) = (1,3) = (1,2)(1,3)(2,3)$
- $(1,3,5) = (1,3)(1,5)$
- $(1,2,3,4) = (1,2)(1,3)(1,4)$

We shall see, however, that if a permutation factors as a product of an odd number of transpositions, then any other factorization of it also involves an odd number of transpositions. Ditto for even numbers of transpositions.

3. Since every permutation can be factored as a product of disjoint cycles, we conclude

Proposition 0.1. *Every permutation $f \in \mathbb{S}_n$ can be factored as a product of transpositions, generally in many different ways.*

For example, in $\mathbb{S}_8$ we have

$$(1,3,5)(2,4,6,8) = (1,3)(1,5)(2,4)(2,6)(2,8) \ .$$

This permutation will soon be called odd; and it does require an odd number of transpositions.

Remark. This factorization essentially says that any shuffle of a deck of cards can be achieved by repeatedly swapping two cards at a time. This is quite believable.

4.

Definition 0.2. *Let f be any permutation in $\mathbb{S}_n$; and suppose when f is written as a product of disjoint cycles that we require d such cycles,* including *all* 1*-cycles. Then the* sign *of f is*

$$\operatorname{sgn}(f) = (-1)^{n-d} \ .$$

If $\operatorname{sgn}(f) = +1$*, we say that f is an* even *permutation; if* $\operatorname{sgn}(f) = -1$*, we say that f is* odd.

The Gap lingo is

```
gap> SignPerm(f);
```

5. **Examples**. Remember to count all 1-cycles, which normally we would suppress for ease of reading.

   - the identity $e = () = (1)(2)\dots(n)$ has $d = n$ one-cycles hence
   $$\mathrm{sgn}(e) = (-1)^{n-n} = +1\ .$$
   - A transposition $t = (a, b)$ has a single 2-cycle and $n - 2$ one-cycles,
   so $d = 1 + (n - 2) = n - 1$, so
   $$\mathrm{sgn}(t) = (-1)^{n-(n-1)} = -1\ .$$
   individual transpositions are odd
   - Since the m-cycle $c = (a_1, \dots, a_m) = (a_1, a_2)(a_1, a_3)\cdots(a_1, a_m)$, the sign of an m-cycle c is
   $$\mathrm{sgn}(c) = (-1)^{n-(1+n-m)} = (-1)^{m-1}\ .$$

   Thus, a little confusingly, a 5-cycle is even, whereas a 6-cycle is odd.

The crucial result is a neat calculation:

Proposition 0.3. *For any permutation f and transposition $t = (a, b)$ in $\mathbb{S}_n$,*
$$\mathrm{sgn}(ft) = -\mathrm{sgn}(f) = \mathrm{sgn}(f)\mathrm{sgn}(t)\ .$$

Proof. Write f as a product of disjoint cycles, taking care to include all 1-cycles:
$$f = (\dots)\cdots(\dots)(\dots)\cdots(\dots)\ .$$
The distinct elements a and b must appear somewhere and exactly once, either in a common cycle or in different cycles.

Case 1. A common cycle. We convey the same mapping information by moving a to the front of the cycle. The rest of the cycle must look something like
$$(a, x_1, \dots, x_l, b, y_1, \dots, y_k)\ .$$

(Possibly $l = 0$ so there aren't any x's, etc.; this won't hurt our argument.) Anyway, this cycle for f is disjoint from all other cycles, so we can commute it to the end to get

$$f = (\ldots)\cdots(\ldots)(\ldots)\cdots(a, x_1, \ldots, x_l, b, y_1, \ldots, y_k)\ ,$$

whence

$$\begin{aligned} ft &= (\ldots)\cdots(\ldots)(\ldots)\cdots(a, x_1, \ldots, x_l, b, y_1, \ldots, y_k)\cdot(a, b) \\ &= (\ldots)\cdots(\ldots)(\ldots)\cdots(a, x_1, \ldots, x_l)(b, y_1, \ldots, y_k)\ , \end{aligned}$$

thereby introducing exactly one more cycle! The number of disjoint cycles goes up by 1; since this appears in the exponent in the definition of the sign, the sign must change by the factor -1.

Case 2. a and b in different cycles. This is similar and basically reverses the calculation in Case 1. Now the number of disjoint cycles goes down by 1; but again this multiplies the sign by -1.

□

6.

Theorem 0.4. *The function*

$$\begin{aligned} \mathrm{sgn} : \mathbb{S}_n &\to \{\pm 1\} \\ f &\mapsto \mathrm{sgn}(f) \end{aligned}$$

is a homomorphism from the group $\mathbb{S}_n$ (with permutation composition) to the group $\{\pm 1\}$ of order 2 (now multiplication of integers). In other words, we have

$$\mathrm{sgn}(fg) = \mathrm{sgn}(f)\mathrm{sgn}(g)$$

for all $f, g \in \mathbb{S}_n$.

Proof. Any f and g can be written as a product of transpostions, say $f = t_1 t_2 \cdots t_k$ and $g = \tilde{t}_1 \cdots \tilde{t}_l$. By repeatedly applying Proposition 0.3, we get

$$\begin{aligned} \mathrm{sgn}(f) &= \mathrm{sgn}([t_1 \cdots t_{k-1}]t_k) \\ &= (-1)\mathrm{sgn}(t_1 \cdots t_{k-1}) \\ &= (-1)^2\mathrm{sgn}(t_1 \cdots t_{k-2}) \\ &= (-1)^k\mathrm{sgn}(e) \\ &= (-1)^k. \end{aligned}$$

Similarly, $\mathrm{sgn}(g) = (-1)^l$, so that

$$\mathrm{sgn}(fg) = \mathrm{sgn}(t_1 t_2 \cdots t_k \tilde{t}_1 \cdots \tilde{t}_l) = (-1)^{k+l} = (-1)^k(-1)^l = \mathrm{sgn}(f)\mathrm{sgn}(g) \ .$$

□

7.

Corollary 0.5. *Parity of permutations has a new, sensible meaning. An even permutation can be factored only as an even number of transpositions; an odd permutation can be factored only as an odd number of transpositions.*

Proof. Note that $(-1)^k = +1$ forces k to be even, never odd.

□

8. **Application 1 - determinants**. Suppose $A = [a_{ij}]$ is an $n \times n$ matrix. One way to define the determinant is

$$\det(A) := \sum_{f \in \mathbb{S}_n} \mathrm{sgn}(f) \ a_{1,(1)f} a_{2,(2)f} \cdots a_{n,(n)f} \tag{1}$$

(a sum of $n!$ signed terms, each a product of n specially selected entries).

Remark. This definition makes sense over any field, in fact, over any commutative ring R with identity 1.

9. **Application 2 - the '15-puzzle'**. This familiar puzzle has 15 sliding blocks labelled $1, \ldots, 15$ and located in a 4×4 frame. The 16th square is empty or blank, so we label it b. By sliding the blank around, we can reconfigure the blocks in various ways.

   Here is the starting configuration:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

   The key problem is this: can we slide the blocks so as to arrive at

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

   Solution. No, we cannot. Each unit move of the blank space (either horizontal or vertical) leaves most of blocks fixed and really amounts to applying a transposition of the form (i, b), where $i \in \{1, 2, \ldots, 15\}$. Any succession of m such moves amounts to a product of m transpositions, whose sign is $(-1)^m$ (Theorem 0.4). However, the blank space is still at the lower right corner, which means that we have moved the blank an even number of times (both horizontally and vertically). In any case, m must be even. Thus we have effected an even permutation on the set $\{1, 2, \ldots, 15, b\}$. The configuration in the second figure amounts to the transposition $(1, 2)$, which is odd. $\square$

10. **Application 3 - the Alternating Group**.

Definition 0.6. *The* alternating group of degree n *is the set* $\mathbb{A}_n$ *of all even permutations in* $\mathbb{S}_n$*, still with left to right composition.*

(a) **Remarks**. Thus $\mathbb{A}_n$ is the *kernel* of the homomorphism sgn in Theorem 0.4. Its order is $\frac{n!}{2}$.

(b) For example, $\mathbb{A}_3$ is isomorphic to the group of rotational symmetries of an equilateral triangle (order 3, rotations through $0°, +120°, -120°$).

(c) Likewise, $\mathbb{A}_4$ faithfully represents the group of rotational symmetries of a regular tetrahedron in ordinary space. There are 12 rotations:

- the identity rotation (through 0°), corresponding to the identity permutation $()$.
- four 120° rotations (looking from outside onto a triangular face), corresponding to say $(1,2,3), (1,4,2), (1,3,4), (2,4,3)$.
- four $-120°$ rotations (still looking from outside onto a triangular face), corresponding to say $(1,3,2), (1,2,4), (1,4,3), (2,3,4)$.
- three 180° rotations, corresponding to $(1,2)(3,4)$, $(1,3)(2,4)$ and $(1,4)(2,3)$.

We have twelve symmetries that we can achieve by physically manipulating the tetrahedron; and we have twelve even permutations.

In fact, we have listed the four conjugacy classes of $\mathbb{A}_4$. On the geometrical side, the motions in each class have the 'same geometric effect' on the tetrahedron. In particular, 120° rotations and $-120°$ are different: we cannot pass from one to the other without the use of a reflection taking right to left hand. But such reflections must correspond to odd permutations of the four vertices.

In parallel to that, the permutations in each conjugacy class 'look like one another'. In addition, we have seen that we do further have to distinguish say $(1,2,3)$ from its inverse $(1,3,2)$ when the setting is $\mathbb{A}_4$. However, when the setting is enlarged to $\mathbb{S}_4$ these two classes fuse into one.

(d) Let's see how this plays out in Gap:

```
gap> S4:=SymmetricGroup(4);;
gap> A4:=AlternatingGroup(4);Size(A4);
Alt( [ 1 .. 4 ] )
12
gap> IsSubgroup(S4,A4);
true
gap> conA:=ConjugacyClasses(A4);;Size(conA);
4
gap> for j in [1..4] do Print(j," ",Elements(conA[j]),"\n");od;
1 [ () ]
2 [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]
3 [ (2,4,3), (1,2,3), (1,3,4), (1,4,2) ]
4 [ (2,3,4), (1,2,4), (1,3,2), (1,4,3) ]
gap> conS:=ConjugacyClasses(S4);;Size(conS);
5
gap> for j in [1..5] do Print(j," ",Elements(conS[j]),"\n");od;
1 [ () ]
2 [ (3,4), (2,3), (2,4), (1,2), (1,3), (1,4) ]
3 [ (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]
4 [ (2,3,4), (2,4,3), (1,2,3), (1,2,4), (1,3,2), (1,3,4), (1,4,2),
  (1,4,3) ]
5 [ (1,2,3,4), (1,2,4,3), (1,3,4,2), (1,3,2,4), (1,4,3,2), (1,4,2,3)
```

Thus the $4! = 24$ elements of $\mathbb{S}_4$ lie in 5 classes. For example, the second class consists of the six reflection symmetries. The fourth class consists of the rotations of period 3 - now they are all alike since the presence of reflections lets the group waive the distinction between clockwise and anticlockwise. The second class is unchanged (and a clockwise 180° rotation is indeed identical to an anticlockwise 180° rotation).

This leaves the last class, consisting of all six 4-cycles in the symmetric group. (Recall that a 4-cycle is an odd permutation.) These must correspond to a symmetry for the tetrahedron which (like reflections) reverses orientation. In other words, such symmetries would send a left hand sketched on the surface of the solid to a right hand.

So look at a 4-cycle like $(1, 2, 3, 4)$. What does this mean geometrically? It will help to hold a model in your hand, with an edge horizontal and the opposite edge also horizontal but ‘perpendicular’ to the first. Imagine the vertical *axis* passing through the midpoints of these two opposite edges. The symmetry that we are after here is a composite thing obtained by composing a 90° turn about the vertical axis with a subsequent reflection in the (horizontal) plane perpendicular to the axis and through the centre of the tetrahedron. (Caution: this last reflection on its own is not a symmetry, nor is the 90° turn!) If you track the effect of this symmetry, you will see that it cyclically sends the 4 vertices of the tetrahedron along a ziz-zag path through the edges. (Such a path is called a *Petrie polygon* for the tetrahedron.) Thus we recreate the 4-cycle in a geometrical way.

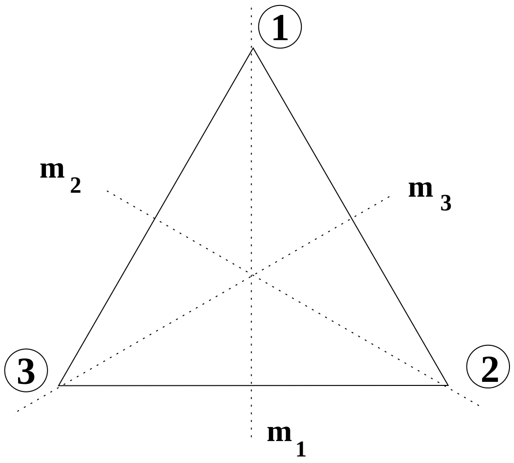
This sort of combined reflection-rotation is called a *rotatory reflection*. It certainly reverses sense, since the reflection part does but the rotation part does not. Yet it is different from an ordinary relection. An ordinary reflection fixes all points on its planar mirror; a rotatory reflection fixes only one point, in this case the centre of the tetrahedron. This qualitative geometrical distinction translates into distinct conjugacy classes in the group $\mathbb{S}_4$.

One Group from Several Points of View

1. **Geometrical Symmetry**: let G be the group of symmetries for an equilateral triangle. We know that there are three rotations, including the identity, say $1, s_1, s_2$, together with three reflections r_1, r_2, r_3. Thus

   $$G = \{1, s_1, s_2, r_1, r_2, r_3\} \ ,$$

   with left-to-right composition as usual. Note that r_j is the reflection in mirror m_j. Of course, $|G| = 6$.

   Exercise. Write out the multiplication table for G. Remember that fg means first apply the isometry f to the triangle, then the isometry g.

2. **Permutations**: label the vertices of the triangle $1, 2, 3$. Since each isometry of the plane is determined by its effect on this triangle, we can unambiguously track the isometries via permutations of $\{1, 2, 3\}$. We obtain the permutation group

   $$\mathbb{S}_3 = \{(\,), (1,3,2), (1,2,3), (2,3), (1,3), (1,2)\}$$

   (again composed left-to-right as functions).

   We have seen that $G \simeq S_3$. Explicitly, there is an isomorphism mapping

$$\begin{array}{rcl} G & \to & \mathbb{S}_3 \\ 1 & \mapsto & (\,) \\ s_1 & \mapsto & (1,3,2) \\ s_2 & \mapsto & (1,2,3) \\ r_1 & \mapsto & (2,3) \\ r_2 & \mapsto & (1,3) \\ r_3 & \mapsto & (1,2) \end{array}$$

3. **Matrices (version 1) : orthogonal**. Place the origin O at the centre of the triangle. Thus every symmetry of the triangle fixes O.

   Compute relative to the usual **orthonormal** basis. After rescaling the triangle, we may assume that the top vertex is

   $$\mathbf{e_2} = [0,1] \quad .$$

   As usual,

   $$\mathbf{e_1} = [1,0]$$

   is the unit vector pointing east. (It extends outside the triangle a little.) We then get a matrix group $M1$ in which the above isometries are represented in order as

   $$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{bmatrix}, \begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix},$$

   $$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1/2 & -\sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{bmatrix}, \begin{bmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix} \quad .$$

   Here each matrix is orthogonal: to get the inverse, simply transpose.

4. **Matrices (version 2) : nice but not orthogonal**

   We can actually employ any basis that we want. But it makes sense to choose a 'nice' basis. So let's take vertices 1 and 2 of the triangle as the new basis vectors $\mathbf{d_1}$ and $\mathbf{d_2}$. Because the triangle is equilateral, we see that vertex 3 is given by $-\mathbf{d_1} - \mathbf{d_2}$. A little computation gives a new set $M2$ of matrices for the original isometries, again in the original order:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \ .$$

Thus the entries of these new matrices are a little nicer to work with.

We have the same group, of course; but since the basis is non-standard, the corresponding coordinates are non-standard and measurement works differently. For example, the usual inner product $x_1y_1 + x_2y_2$ using new coordinates *does not* usefully measure anything.

5. The **trace** of a square matrix A is the sum of its diagonal entries, say

$$\mathrm{tr(A)} := \sum_{\mathrm{j}} \mathrm{a_{jj}} \ .$$

Thus the trace of a matrix is a very special scalar.

6. Notice that corresponding matrices in the above groups have identical traces. Why is this so?

Well, we have changed basis according to this rule:

$$\mathbf{d_1} = \mathbf{e_2} = 0\mathbf{e_1} + 1\mathbf{e_2} \ , \ \ \mathbf{d_2} = (\sqrt{3}/2)\mathbf{e_1} + (-1/2)\mathbf{e_2} \ .$$

Thus the corresponding *basis change matrix* is

$$B = \begin{bmatrix} 0 & 1 \\ \sqrt{3}/2 & -1/2 \end{bmatrix} \ .$$

Symbolically we should think

(new basis $\mathbf{d_1}, \mathbf{d_2}$ in a column) $= B$ (old basis $\mathbf{e_1}, \mathbf{e_2}$ in a column).

It follows that if A is one of the six 'old' matrices in $M1$, then the corresponding 'new' matrix in $M2$ is

$$BAB^{-1} .$$

Remark: Getting the matrices arranged in the correct way here is a little tricky. Of course, much the same procedure works in n dimensions.

7. Let's return to the traces. It is easy to check for square $n \times n$ matrices A and C that

$$\mathrm{tr(AC)} = \mathrm{tr(CA)} .$$

(Do this as an exercise.) Thus

$$\begin{aligned} \mathrm{tr((BA)B^{-1})} &= \mathrm{tr(B^{-1}(BA))} \\ &= \mathrm{tr((B^{-1}B)A)} \\ &= \mathrm{tr(IA)} \\ &= \mathrm{tr(A)} . \end{aligned}$$

In short, basis change does not change the trace values for matrix group representations of the original group G.

These trace values are called the **character values** for the matrix representation. Indeed, they serve to classify and distinguish essentially different matrix representations for one and the same group G.

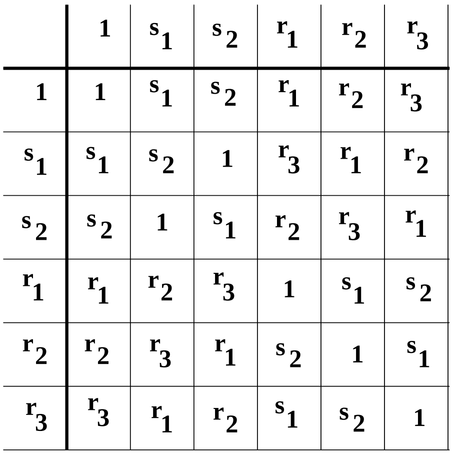
In a sense, the character values (traces) contain just enough numerical information to completely determine the matrix group (up to a change in basis). All other numerical data in the matrices is clutter.

8. **Exercise**. Prove that conjugate elements in G must have identical character values.

The upshot, which is quite hard to prove, is that a matrix group is determined by k scalars, where k is the **class number** = number of conjugacy classes in G.

9. **A first level of abstraction: the multiplication table of G**

   In a basic way, the multiplication table alone completely defines G, though we must of course inspect the table to root out the interesting properties of G. In this abstract point of view, we forget all concrete representations such as isometries, permutations, matrices, etc. and think merely of $|G|$ symbols combined according to the table.



	1	s_1	s_2	r_1	r_2	r_3
1	1	s_1	s_2	r_1	r_2	r_3
s_1	s_1	s_2	1	r_3	r_1	r_2
s_2	s_2	1	s_1	r_2	r_3	r_1
r_1	r_1	r_2	r_3	1	s_1	s_2
r_2	r_2	r_3	r_1	s_2	1	s_1
r_3	r_3	r_1	r_2	s_1	s_2	1

10. **The second and universal level of abstraction: a presentation for G.**

    Intuitively, a *presentation* for a group G is a 'concise' summary of the multiplication table, basically a minimal amount of information which would suffice to reconstruct the whole table. Note that this means that

    - we should be able to reconstruct all elements of the group; and
    - we should be able to say how all elements multiply.

Now let's be more precise. What we require in a presentation is

(a) a (preferably small) set of **generators** $a, b, c, \ldots$ for the group G. This means that *every* element $g \in G$ is a product of these generators or their inverses, allowing repeats. We noted earlier that such a product is often called a **word** in the generators. Examples are $a, aa^{-1}, abaaab^{-1}b^{-1}cc$ etc. Of course, these can sometimes be simplified using the basic laws of exponents valid for *all* groups:

$$aa^{-1} = 1 \ , \ abaaab^{-1}b^{-1}cc = aba^3b^{-2}c^2 \ .$$

But there could well be other simplifications possible due to special features of the group G in question. These peculiarities are given by

(b) a set of **relations** (a.k.a. relators) satisfied by the given generators and from which all valid relations in G follow by algebraic manipulations in the group. This is a little hard to define more precisely, so here we will just sketch a few examples and state the key theorems.

11. **Example**. Suppose in the calculation just above, we do know that $ab = ba$, which can be rewritten as $aba^{-1}b^{-1} = 1$. Then we achieve a further simplification:

$$abaaab^{-1}b^{-1}cc = a^4b^{-1}c^2 \ .$$

12. **Example**. Suppose G is generated by *two* elements a, b which satisfy the relations

$$a^2 = b^2 = (ab)^3 = 1 \qquad (**)$$

Various different groups have these generators and satisfy the relations!!

(a) $a = b = 1$ (say the integer 1); so $G = \{1\}$ has order 1.

(b) $a = b = -1$ (again integers). Check that the relations (**) are satisfied. What now is the order of G?

(c) Another possibility using ordinary integers? $a = 1$ and $b = -1$. Are all the relations (**) above satisfied?

(d) Now try the symmetry group of the equilateral triangle above. Let $a = ?$ and $b = ?$ be carefully chosen symmetries. Do they generate the full symmetry group? Do they satisfy the relations (**)?
Hint: your choices for a and b will be closely guided by the relations to be satisfied.

(e) Thus the order of G could be as big as 6. Could it be larger still? Try to compute the possibilities!! Take all possible combinations of a, b, a^{-1}, b^{-1}, subject to the relations (**), and determine how many truly different elements you can get. For example, $a^2 = 1$ implies $a^2a^{-1} = 1a^{-1}$, so that $a = a^{-1}$. In short, *in this example*, negative powers of the generators are unnecessary, and at the outset, we can restrict only to positive integral exponents.

(f) In fact, there is a *largest such group* satisfying (**) !! And its order is __________

Remark: the peculiar structure of the relations in (**) means that the symmetry group of the equilateral triangle is the *Coxeter group* of type A_2.

13.

Theorem 0.7.

Consider all groups generated by generators

$$a, b, c \ldots$$

satisfying specified relations

$$w_1 = w_2 = \ldots = 1$$

(namely certain special words in the generators).

Then there exists a 'largest' such group, denoted

$$G = \langle a, b, c \ldots \mid w_1 = w_2 = \ldots = 1 \rangle$$

(This is called a *presentation* for the group G.)

More precisely, if H is any other group with corresponding generators $\tilde{a}, \tilde{b}, \tilde{c} \ldots$ satisfying the corresponding relations $\tilde{w}_1 = \tilde{w}_2 = \ldots = \tilde{1}$, then there exists a unique homomorphism

$$\varphi : G \to H$$

which explicitly sends a to $\tilde{a}$, b to $\tilde{b}$, etc.

14. **Remarks**.

(a) This is a very powerful theorem. For example, it says that we can construct groups at will, choosing random symbols for generators, random equations for relations. Of course, the resulting groups could be trivial (order 1), could be infinite, could be uninteresting.

(b) Recall that $H \simeq G / \ker \varphi$. Hence,

$$|G| = |H| \, |\ker \varphi| \ .$$

Since $|H|$ divides $|G|$, we do indeed find that $|G| \geqslant |H|$. In this sense, G is the largest group satisfying the relations. (It could be infinite.)

(c) It is a nice exercise to use the theorem to prove that G is uniquely defined up to isomorphism.

15. **Exercises on presentations**. Compute the orders of these groups and describe each in more familiar terms (e.g. symmetry group of equilateral triangle).

    (a) $G = \langle a \mid a^2 = 1 \rangle$

    (b) $G = \langle b \mid b^3 = 1 \rangle$

    (c) $G = \langle a, b \mid a^2 = b^2 = (ab)^4 = 1 \rangle$

    (d) $G = \langle a, b \mid a^2 = b^4 = aba^{-1}b^{-1} = 1 \rangle$

    (e) $G = \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^3 = (bc)^3 = (ac)^2 = 1 \rangle$

    (f) $G = \langle a, b \mid a^2 = b^2 = (ab)^2 \rangle$
    Warning: we aren't saying $a^2 = 1$ here; rather, the relations are just clean ways of writing

    $$a^2 b^{-2} = a^2 (ab)^{-2} = 1 \ \ .$$

    It is still possible, for example, that a has infinite period!!

    (g) $G = \langle a, b \mid a^2 = b^2 = 1 \rangle$

    (h) $G = \langle a, b \mid a^3 = b^3 = (ab)^3 = 1 \rangle$

Counting with and in Permutation Groups

1. What we have to say here can be phrased in the slightly more general context of *actions*. We may return to this later, particularly since 'actions' are a key device in GAP.

   Definition 0.8. *Let G be a group and X any set. In a formal sense, an* action of G on the set X *is any homomorphism*

   $$\varphi : G \to \mathbb{S}_X \ .$$

   Here is how we express computations with actions in a more congenial way. For any group element $g \in G$ and set element $x \in X$, we have that $(g)\varphi$ is a permutation (in $\mathrm{Im}(\varphi)$, a subgroup of $\mathbb{S}_X$). Thus $x^{(g)\varphi}$ makes sense. As long as φ is understood from context, we can suppress φ with the more economical notation

   $$x^g := x^{(g)\varphi}, \text{ for all } x \in X \text{ and } g \in G \ .$$

   You should verify these very nice rules:

   - $x^1 = x$ for all $x \in X$. Here 1 is the identity in G, of course.
   - $x^{gh} = (x^g)^h$, for all $x \in X$ and $g, h \in G$. Here we write the operation in G multiplicatively, of course.

   Remark. Actually we have above a right-action by G on X. With a bit of care, one can also define left actions, written ${}^g x$.

2. For now we put aside general actions and simply

   assume G is a subgroup of the permutation group $\mathbb{S}_X$.

   Usually we will have $X = \{1, \ldots, n\}$ for some integer $n \geqslant 1$.

3.

Definition 0.9. *(a) If $a \in X$ then the G-*orbit *of a is*

$$\mathrm{Orb}_G(a) := \{a^g : g \in G\}.$$

This subset of X consists of all places we can get to from 'a' under the action of G.

(b) The group G is transitive *on X if $\mathrm{Orb}_G(a) = X$ for some $a \in X$ (and hence for* <u>*any*</u> *$b \in X$).*

*(c) If $a \in X$ then the G-*stabilizer *of a is*

$$\mathrm{Stab}_G(a) := \{g \in G : a^g = a\}$$

4. Prove yourself that

Theorem 0.10. *The orbits of G on X* partition *the set X.*

5.

Theorem 0.11. *Let $a \in X$. Then*

(a) $\mathrm{Stab}_G(a)$ is a subgroup of X.

(b) Let T be a transversal to $\mathrm{Stab}_G(a)$ in G. Then the map

$$\begin{array}{rcl} \varphi : T & \to & \mathrm{Orb}_G(a) \\ t & \mapsto & a^t \end{array}$$

is a bijection. Thus the elements of an orbit are in 1–1 correpondence with the right cosets (say) of the stabilizer of an element in the orbit. Furthermore, if G is finite then

$$|\mathrm{Orb}_G(a)| = \frac{|G|}{|\mathrm{Stab}_G(a)|} .$$

(The orbit size must be a divisor of the group order.)

(c) If also $b \in \mathrm{Orb}_G(a)$, i.e. if $b = a^k$ for some particular $k \in G$, then the map

$$\begin{array}{rcl} \psi : \mathrm{Stab}_G(a) & \to & \mathrm{Stab}_G(b) \\ g & \mapsto & k^{-1}gk \end{array}$$

is a group isomorphism.

Remark. We say that $\mathrm{Stab}_G(a)$ and $\mathrm{Stab}_G(b) = k^{-1}\mathrm{Stab}_G(a)k$ are *conjugate* subgroups of G.

6.

Definition 0.12. *Suppose X is finite and $G \leqslant \mathbb{S}_X$. For each $g \in G$ we let*

- $\mathrm{Fix}(g) := \{x \in X : x^g = x\}$
- $\theta(g) = |\mathrm{Fix}(g)|$.

In other words, $\theta : G \to \mathbb{Z}^{\geqslant 0}$; and $\theta(g)$ is simply the number of points fixed by g as it acts on X. For example, if $X = \{1, \ldots, n\}$ and $g = ()$, then $\theta(g) = n$.

7. Show for $k \in G$ that

$$\mathrm{Fix}(k^{-1}gk) = k^{-1}\mathrm{Fix}(g)k\ .$$

We might write this last product of sets as $[\mathrm{Fix}(g)]^k$. Note that this new set has the same size as $\mathrm{Fix}(g)$. Why?

8. Prove that θ is a *class function* on G, i.e. is constant on conjugacy classes. In other words, for all $g, k \in G$ we have

$$\theta(g) = \theta(k^{-1}gk)\ .$$

9.

Theorem 0.13. (Burnside's Orbit Formula) *The number of distinct G-orbits as G acts on X is*

$$\frac{1}{|G|}\sum_{g \in G}\theta(g)$$

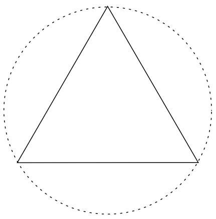
(i.e. the 'average number of fixed points' over the whole group).

10. Exercise. How many 'essentially distinct' necklaces can be made with n beads, either black or white but otherwise identical?

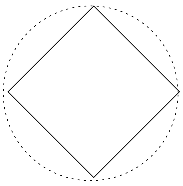
The symmetry groups for polygons, polyhadra, polytopes of the most symmetric kind

1. For an integer $n \geqslant 2$, suppose $v_1, \ldots, v_n$ are equally spaced points on a circle. Connect these in cyclic order by edges $e_j = [v_j, v_{j+1}]$, for $1 \leqslant j \leqslant n$, taking subscripts modulo n. Thus e_n closes the cycle by connecting v_n to v_1.

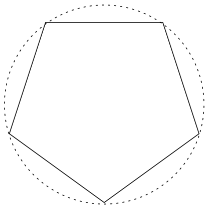
   We obtain a *regular n-gon*, denoted $\{n\}$:



{3}

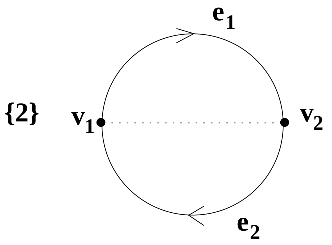


{4}



{5}

But what if n = 2?



2. Suppose $n \geqslant 3$. We see that $\{n\}$ is a familiar convex polygon. After replacing each edge by the circular arc it spans, we obtain *circular n-gons* with the same abstract structure. (Think of the vertices and edges as defining a *graph*.)

   It therefore makes sense to say that the *digon* $\{2\}$ (see the figure above) has two vertices and two edges. We just cannot separate the edges if we insist on using straight line segments.

3. What is the symmetry group $\mathbb{D}_n$ of the regular polygon $\{n\}$?

   The mirrors for the various reflection symmetries are lines, all passing through the centre O of the circumscribing circle. These mirrors divide the plane into angular regions. The number of such regions will equal the order of the symmetry group.

Definition 0.14. *For $n \geqslant 2$, the symmetry group of a regular n-gon $\{n\}$ is denoted $\mathbb{D}_n$.*

Warning. There is much disagreement about whether the subscript n should be a little different (see below). I myself agree with those who disagree.

4. We have observed for the equilateral triangle and the square that we get generating reflections by taking two distinct mirrors separated by the smallest possible angle. For an $\{n\}$, this angle will be π/n.

   To make the process a little more susceptible to generalization in higher dimensions, let us do the following. A *flag* of the polygon is a pair consisting of an incident vertex and edge. (It will turn out that the order of the symmetry group $\mathbb{D}_n$ equals the number of such flags. Of course, this order equals $2n$, since every vertex lies on 2 edges. Some authors, including at other times myself, use the order $2n$ as subscript, instead of n itself.)

   So choose any one flag as your *base flag*, say (v_1, e_1) to be specific. Let

   - r_0 be the reflection in the perpendicular bisector of edge e_1. Thus

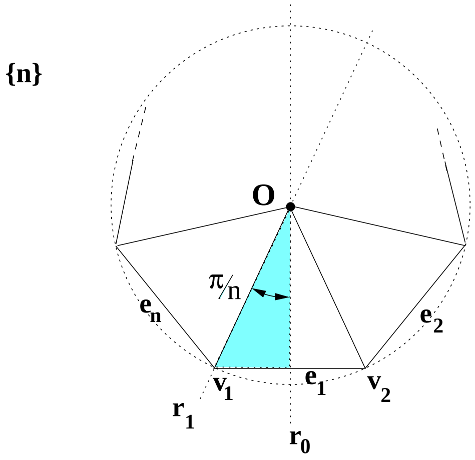
     $$\begin{aligned} r_0 \quad : \quad & v_1 \to v_2 \\ & e_1 \to e_1 \end{aligned}$$

     In short, r_0 moves the 0-dimensional 'face' (= vertex) of the base flag and fixes the 1-dimensional face (= edge). (As one entity, edge e_1 is fixed; of course, it is flipped end-for-end in the process.)

   - r_1 be the reflection in the line joining O to v_1. Thus

     $$\begin{aligned} r_1 \quad : \quad & v_1 \to v_1 \\ & e_1 \to e_n \end{aligned}$$

     In short, r_1 moves the 1-dimensional 'face' (= edge) of the base flag and fixes the 0-dimensional face (= vertex).



A *fundamental region* for the action of the symmetry group $\mathbb{D}_n$ on the polygon $\{n\}$ has been shaded in. Repeated application of r_0 or r_1 will move this region to all $2n$ available positions.

Thus $\mathbb{D}_n$ has generators r_0, r_1; once again we see that the order is $2n$.

The group $\mathbb{D}_n$ is called *dihedral* since we imagine it generated by two reflections. In fact, we can make an actual *kaleidoscope* corresponding to this group by using two real mirrors.

5. A presentation for $\mathbb{D}_n$.

We can reason as we did for the equilateral triangle or square: explicitly list the $2n$ elements of the group. Alternatively one can use coset enumeration on the trivial subgroup. In any case, a presentation is

$$\mathbb{D}_n : \langle\, r_0, r_1 \mid r_0^2 = r_1^2 = (r_0 r_1)^n = 1 \rangle$$

This sort of presentation means that $\mathbb{D}_n$ is an example of a *Coxeter group*. These groups appear all throughout mathematics, often in places which wouldn't seem to have much to do with polygons or polyhedra.

6. Exercises.

   (a) Fix a background label 'j' next to vertex v_j for each j. Use this to represent the generators r_0 and r_1 as permutations R_0, R_1 on $\{1, \ldots, n\}$.

   Compute R_0R_1 in this representation. For which n is the resulting group $\langle R_0, R_1\rangle$ of permutations isomorphic to $\mathbb{D}_n$? In other words, can the permutations ever fail us?

   (b) Clearly $\langle R_0, R_1\rangle$ is a subgroup of $\mathbb{S}_n$. Can the subgroup equal the whole group for any n?

   (c) What goes wrong with the above permutations when $n = 2$? Correct that to give a *faithful* permutation representation of $\mathbb{D}_2$, say as a subgroup of $\mathbb{S}_4$.

   (d) Compute on geometrical grounds the number of conjugacy classes in $\mathbb{D}_n$. (Intuitively, a conjugacy class consists of all symmetries which act in the 'same' geometrical way on the n-gon. Here 'same' will mean 'up to relocation via any and all elements of the surrounding group, here $\mathbb{D}_n$.)

   Find out how to retrieve a permutation version of $\mathbb{D}_n$ in GAP and check your conjectures about the number of conjugacy classes for several small values of n.

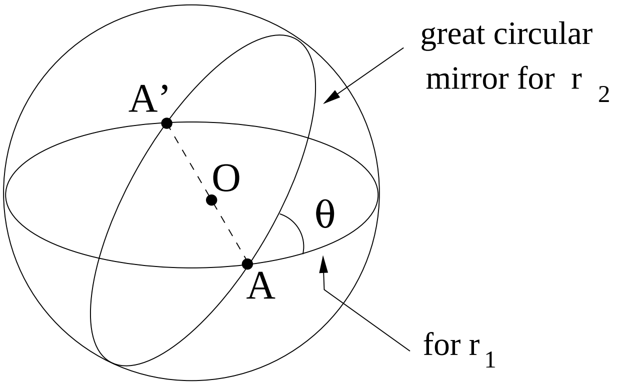
   Which subscript convention does GAP adhere to?

The Finite reflection groups G

Our examples indicate that regular polygons and polyhedra, and presumably their higher dimensional kin, have symmetry groups generated by reflections. We survey these groups in ordinary space.

7. Suppose then that G is a *finite group generated by reflections* in $\mathbb{R}^3$ and pick any point P. Its orbit, $\mathrm{Orb}_G(P)$, is finite, since G is finite. The orbit therefore has a well-defined centroid O.

   But since G consists of isometries, each of which rearranges the points in the orbit, it must be that O is *fixed by every element of the group.* Furthermore, since G consists of isometries, this means that G fixes as an entity any sphere centred at O. In short, we can track the action of G by examining how it acts on the unit sphere $\mathbb{S}^2$ centred at O:

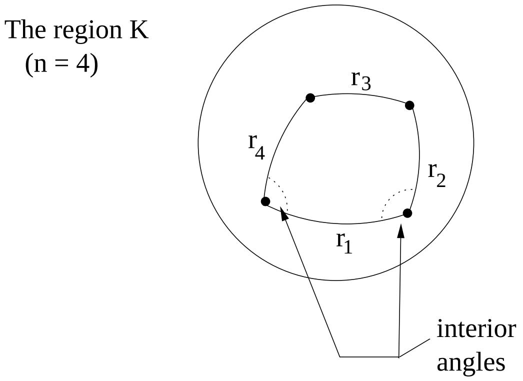


   Any reflection in G has a plane mirror passing through O. This mirror meets $\mathbb{S}^2$ in a *great circle.* Two such mirrors intersect in a line which meets the sphere at *antipodal* points A and A', as shown above. Notice that two distinct great circles always intersect in a pair of antipodal points.

   The (dihedral) angle θ from one such mirror to another appears to a spherical bug living on $\mathbb{S}^2$ as an angle on the surface of the sphere. Just as in the Euclidean plane, we find that a product r_1r_2 of reflections equals a rotation through angle 2θ with centre A. If the angle appears to be anticlockwise as we view A from without the sphere, then it will appear clockwise at A'.

8. Now experience with kaleidoscopes informs us that all the mirrors for reflections in G will cut $\mathbb{S}^2$ into various spherical polygons. Any one of these polygons – call it K – serves as a *fundamental region* for the action of the group G. This means that by repeated reflection in the great circles bounding K, we are able to cover the entire sphere once over.

   From another point of view, K is a smallest region *enclosed* by mirrors but not penetrated by any mirror of symmetry. If the polygon K has n sides, let's label the bounding reflections $r_1, \ldots, r_n$ is cyclic order:



9. Look at the reflections r_1, r_2 in two consective sides of K. Suppose the angle from side 1 to side 2 is θ. Then r_1r_2 is a rotation with angle 2θ. Furthermore, $(r_1r_2)^n = 1$ for some integer $n \geqslant 2$. (If $n = 1$ we would have $r_1 = r_2$ and the two mirrors would coincide.)

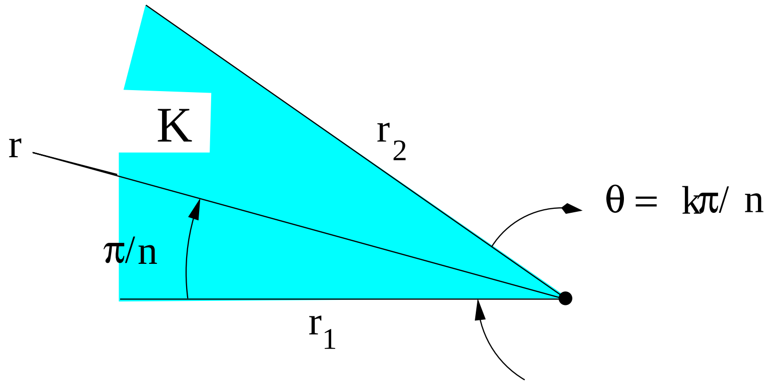
   But $(r_1r_2)^n = 1$ is a rotation, too, now through a multiple of 2π. Thus there is an integer k such that

$$\begin{aligned} n(2\theta) &= 2\pi k \text{ or} \\ \theta &= \frac{k\pi}{n}. \end{aligned}$$

   Put k/n in lowest terms, so that $\gcd(k, n) = 1 = lk - mn$ for certain integers l and m. (This possibly new n will be the period of r_1r_2.) The rotation $g = (r_1r_2)^l$ has angle

$$l(2\theta) = l(2\pi k)/n = 2\pi/n + 2\pi m \equiv 2\pi/n \pmod{2\pi} .$$

Now let r be reflection in the line x located π/n along from the mirror for r_1:



This line is interior to the region K if $k > 1$; but we don't yet know if r is in the group. However, r_1r is also a rotation through $2\pi/n$, so $r_1r = g$ and $r = r_1g$ really is in the group. This contradicts our construction of the region K if $k > 1$.

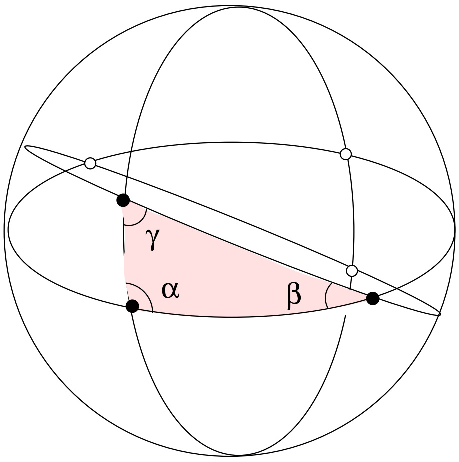
10. **Conclusion**. Each interior angle of K has the form π/n for some integer $n \geqslant 2$ (i.e. is a submultiple of π).

11. **The area of a spherical polygon**

    A *lune* is a region of $\mathbb{S}^2$ bounded by two great semicircles. In the figure on page 39 you can see four lunes terminating at A and A'. Look at the lune specified by the angle θ. The symmetry of the sphere clearly implies that this area is directly proportional to θ. Since the whole unit sphere has area 4π we conclude that

    the area of a lune with polar angle θ is 2θ.

12. Let's look now at a spherical triangle with angles α, β, γ:



Extending its sides we obtain various lunes which intersect in a congruent antipodal triangle (indicated by 'open' vertices). Let A be the area of the triangle. Observing how the various lunes cover the sphere, we get

$$4\pi = 2(2\alpha + 2\beta + 2\gamma) - 4A,$$

so that

the area of a spherical triangle with angles α, β, γ *is*
$\alpha + \beta + \gamma - \pi$*,*
(the angular excess).

13. Let's return to our fundamental region K, which is a spherical n-gon ($n \geqslant 2$) with angles of the form $\frac{\pi}{p_1}, \frac{\pi}{p_2}, \ldots, \frac{\pi}{p_n}$, where we have seen each integer $p_j \geqslant 2$. Now subdivide K into $n-2$ spherical triangles and emply the angular excess. We conclude that

$$K \text{ has area } \pi[\tfrac{1}{p_1} + \cdots + \tfrac{1}{p_n} - (n-2)].$$

But this area is positive. On the other hand, each $\frac{1}{p_j} \leqslant 2$, so that

$$0 < \frac{n}{2} - (n-2)\ .$$

We conclude that $n = 2$ or 3. This immediately leads to an easy enumeration of cases, as well as a formula for the orders of the resulting reflection groups.

14.

Theorem 0.15. *Let G be a finite reflection group in ordinary Euclidean space. Then G belongs to one of the following classes:*

(a) $G = \langle r_1 \rangle$ is generated by one reflection and has order 2. In this case K is a hemisphere.

(b) $G = \langle r_1, r_2 \rangle$ is a dihedral group $\mathbb{D}_p$ for some $p \geqslant 2$. Here G has order $2p$ and K is a lune bounded by semicircles with polar angle π/p.

(c) $G = \langle r_1, r_2, r_3 \rangle$ is generated by three reflections whose mirrors bound a spherical triangle K. The actual cases are

- *$(p_1, p_2, p_3) = (2, 2, p)$ for any integer $p \geqslant 2$. Here G has order $4p$ and can serve as the symmetry group of of a uniform p-gonal right prism.*
- *$(p_1, p_2, p_3) = (2, 3, 3)$. Here G has order 24, is isomorphic to the symmetric group $\mathbb{S}_4$ and serves as the symmetry group of the regular tetrahedron $\{3, 3\}$.*
- *$(p_1, p_2, p_3) = (2, 3, 4)$. Here G has order 48 and can serve as the symmetry group of the cube $\{4, 3\}$ or regular octahedron $\{3, 4\}$. (Here $G \simeq \mathbb{S}_4 \times \mathbb{C}_2$.)*
- *$(p_1, p_2, p_3) = (2, 3, 5)$. Here G has order 120 and can serve as the symmetry group of the regular dodecahedron $\{5, 3\}$ or regular icosahedron $\{3, 5\}$. (G is not isomorphic to $\mathbb{S}_5$; instead $G \simeq \mathbb{A}_5 \times \mathbb{C}_2$.)*

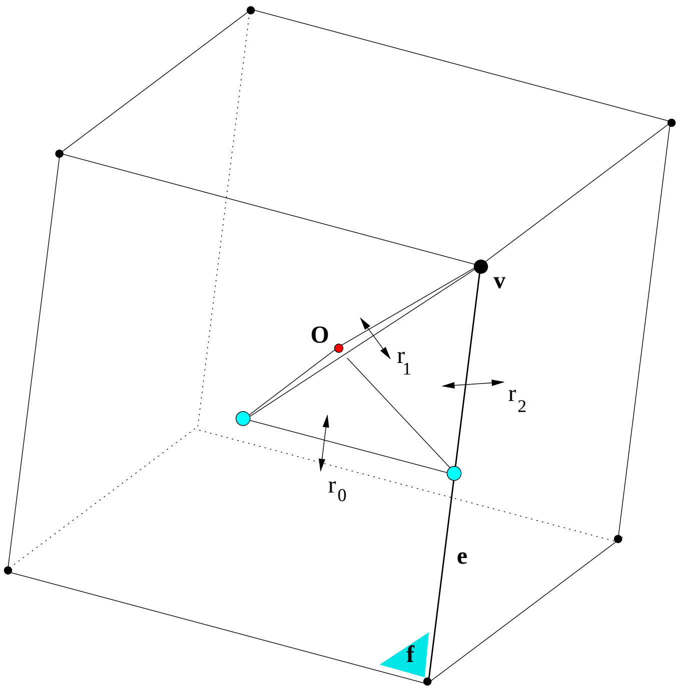
We note that the order of the symmetry group of the regular polyhedron $\{p, q\}$ is

$$\frac{4}{\frac{1}{p} + \frac{1}{q} - \frac{1}{2}} = \frac{8pq}{4 - (p-2)(q-2)} \, .$$

The Abstract Cube

1. The relation between the cube $\mathcal{P}$ and its symmetry group G is quite typical of what happens for general regular polyhedra (regular polytopes of rank $n = 3$). The extension to regular polytopes of higher rank ($n \geqslant 4$) or even to lower ranks (eg. polygons, of rank $n = 2$) is quite natural. Therefore, instead of proving general things, we will just use the cube to suggest a believable description of the basic theory of abstract regular polytopes.

2. The cube has *Schläfli symbol* $\{4, 3\}$ (after Ludwig Schläfli, a 19th century Swiss geometer). Here the '4' indicates that the faces of $\mathcal{P}$ are squares (Schläfli symbol $\{4\}$); the 3 indicates that 3 squares surround each vertex. More precisely, the vertex-figure of a typical vertex like v below is the equilateral triangle $\{3\}$ formed by the three vertices adjacent to v. (Sketch it in yourself.)



3. The group $G = G(\mathcal{P})$ is known to have presentation

$$G = \langle r_0, r_1, r_2 \,|\, r_0^2 = r_1^2 = r_2^2 = (r_0r_1)^{4} = (r_1r_2)^{3} = (r_0r_2)^2 = 1\rangle \; .$$

(You could check the order 48 by coset enumeration. In the 1930's Coxeter used geometric arguments to solidify our understanding of these kinds of groups in all dimensions.) Notice where the 4 and 3 appear. And recall that the period 2 means that r_0 commutes with r_2.

A *Coxeter group* is a group presented in this way as having generators r_j of period 2 subject only to those further relations which specify the periods of products of two distinct generators.

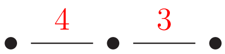
Thus, if there are n generators $r_0, r_1, \ldots, r_{n-1}$, we will have at most $\begin{pmatrix} n \\ 2 \end{pmatrix}$ further defining relations.

Some such relation could be missing. This is an admission that we allow the period to be ∞. For example, the rank 2 Coxeter group

$$\langle r_0, r_1 \,|\, r_0^2 = r_1^2 = 1\rangle$$

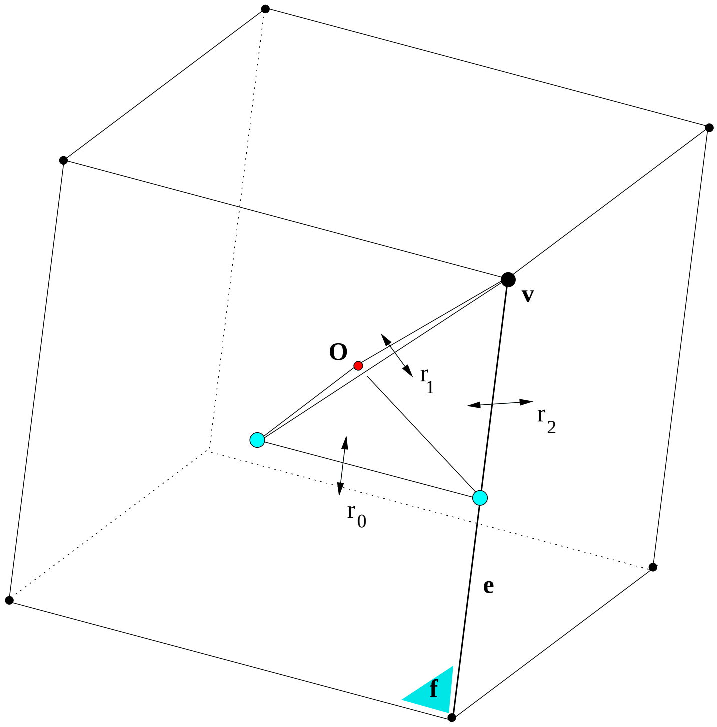
actually is infinite. The generators can be interpreted as reflections in distinct parallel lines in the plane. This gives the symmetry group of the infinite regular polygon $\{\infty\}$ whose vertices are all points with integer coordinates on a line perpendicular to the mirrors. Sketch this yourself, taking care to place the mirrors for r_0, r_1 correctly. You can also see this group portrayed on the door to Tilley 412.

4. The presentation for any Coxeter group can be encoded in a most useful *Coxeter diagram*. The diagram for G above is



The three nodes correspond left-to-right to r_0, r_1, r_2. You can see how the 'rotational' periods are indicated by the branch labels. Crucially, non-adjacent nodes correspond to commuting reflections. This is a very useful trick.

5. Let's return to the picture of the cube:



Now we want to understand how to extract the generating reflections from the geometrical set-up. The first step is to chooses a *base flag*, i.e. an incident [vertex, edge, square face] triple. The flag $[v, e, f]$ is indicated. We may identify each of these components by its centroid. As a result, we get the isosceles right triangle whose vertices are v, the midpoint of e and the centre of f. This triangle does look a bit like a pennant.

There are $48 = 8 \cdot 6$ copies of the pennant on the surface of the cube. We see once more why G has order 48.

If you now join these three points to the body centre O for the cube itself, then you get the framework for an actual *trihedral kaleidoscope*.

The generating reflections now arise in a systematic way:

- reflection r_0 moves only the dim 0 component of the base flag (move v, globally fix e, f as entities);
- reflection r_1 moves only the dim 1 component of the base flag (move e, globally fix v, f as entities);
- reflection r_2 moves only the dim 2 component of the base flag (move f, globally fix v, e as entities).

The base flag is moved by r_j to the so-called $j - adjacent$ flag. Take a moment to find these three flags and shade in their pennants.

Now extract the abstract...

6. In order to count ingredients of each rank, we might emply stabilizers. Observe that

   - the stabilizer of the rank 0 element in the base flag is
   $$G_0 = \mathrm{Stab}_G(v) = \langle r_1, r_2 \rangle$$
   - the stabilizer of the rank 1 element in the base flag is
   $$G_1 = \mathrm{Stab}_G(e) = \langle r_0, r_2 \rangle$$
   - the stabilizer of the rank 2 element in the base flag is
   $$G_2 = \mathrm{Stab}_G(f) = \langle r_0, r_1 \rangle$$

   In brief, the stabilizer of the rank j element in the base flag is
   $$G_j = \langle r_i \, : \, i \neq j, 0 \leqslant i \leqslant n-1 \rangle,$$
   where $n = 3$ for the cube, of course. The same description works for regular polytopes of any rank.

   In any regular polytope $\mathcal{P}$, the symmetry group $G = G(\mathcal{P})$ will be transitive of 'faces' of each particular rank j: there is just one orbit for each. Thus the number of j-faces in $\mathcal{P}$ equals
   $$\frac{|G|}{|G_j|}.$$

7. Now recall how we proved this. We exhibited a $1-1$ correspondence between j-faces and right cosets of the stabilizer in G. If x denotes the j-face in the base flag, then as g runs through G, we have

$$x^g \leftrightarrow G_j g$$

From an abstract point of view: j-faces are the cosets $G_j g$.

8. We have the *ingredients* of $\mathcal{P}$. What about *assembly instructions*? In other words, can we use the cosets to say when some j-face 'lies on' or 'is incident with' some k-face?

Again we look at the cube to see what must happen. For instance, when does a vertex (face of rank $k = 0$) lie on a square (face of rank $j = 2$)?

Well, a typical vertex is v^g and a typical square face is f^h, where $g, h \in G$. Note that g and h might well be different, but due to transitititity, this does cover all cases.

Working in one direction, let us assume that vertex v^g lies on square f^h. Since h^{-1} is a symmetry in G, this means

$$(v^g)^{h^{-1}} = v^{(gh^{-1})} \text{ lies on the base square } f = f^1 = f^{(hh^{-1})}.$$

Now we appeal in an inductive way to our knowledge of lower-rank objects, in this case, the square f whose own symmetry group is isomorphic to $G_2 = \langle r_0, r_1 \rangle$. There must be some $y \in G_2$ such that $v^{(gh^{-1})} = v^y$. This in turn implies that $gh^{-1}y^{-1}$ fixes v, so that $gh^{-1}y^{-1} \in G_0 = \langle r_1, r_2 \rangle$. Thus

$$\begin{aligned} G_0(gh^{-1}y^{-1}) &= G_0 \\ G_0 g &= G_0(yh) \end{aligned}$$

At the same time, since $y \in G_2$, we have $G_2 y = G_2$, so that $G_2 h = G_2(yh)$. This shows that $G_0 g$ and $G_2 h$ have a common representative yh:

$$yh \in G_0 g \cap G_2 h\ .$$

The converse implication is easier. If we assume that $G_k g \cap G_j h$ is non-empty, then say $z \in G_k g \cap G_j h$. In other words, $z = xg$, where x fixes v and $z = yh$, where y fixes f.

Back in the base flag v is incident with f, so that if we apply z we conclude that vertex $v^z = v^{(xg)} = v^g$ is incident with square $f^z = f^{(yh)} = f^h$.

From an abstract point of view: If $k \leqslant j$, the k-face $G_k g$ is incident with the j-face $G_j h$ if and only if

$$G_k g \cap G_j h \neq \emptyset \ .$$

9. We have seen how to 'reconstruct' the cube, at least in combinatorial essentials, purely from the point of view of its symmetry group G.

   Much the same sort of thing is possible for any abstract regular n-polytope, so that many questions concerning polytopes can be reconfigured as questions concerning a suitable group G.

   What sort of groups are suitable? Schulte proved in the early 1980's that the regular n-polytopes correspond in a precise way to *string C-groups* G. Such a group has these properties:

   - it is generated by n specified elements $r_0, \ldots, r_{n-1}$ each of period 2. (The subscripts epmhasize that order is important.)
   - these elements satisfy certain relations
     - $(r_k r_j)^2 = 1$, if $k < j-1$ (indicating commuting generators).
     - $(r_{j-1} r_j)^{p_j} = 1$, for $1 \leqslant j \leqslant n-1$ (think 'rotational periods'). Here each $p_j \in \{2, 3, 4, \ldots, \infty\}$.

     Remarks. We may well need other relations of a type not listed above to effect a presentation. But <u>if</u> no other relations are needed, then the special sort of group that results is called a *Coxeter group with string diagram.* The diagram is a simple left to right string of nodes. If $p_j > 2$, then there is branch labelled p_j connecting the $(j-1)$st node to the jth node.

     The Schläfli symbol for the group (and polytope) is $\{p_1, \ldots, p_{n-1}\}$.

     We are not yet done with special properties for G...

The group must also satisfy an

- *intersection condition*: for any subsets $I, J \subseteq \{r_0, \ldots, r_{n-1}\}$, we have
$$\langle I \rangle \cap \langle J \rangle = \langle I \cap J \rangle \ .$$

  Example. Many of the intersections hold for trivial reaons. In the case of an abstract regular polyhedron (rank $n = 3$), the crucial condition to be checked is
$$\langle r_0, r_1 \rangle \cap \langle r_1, r_2 \rangle = \langle r_1 \rangle \ .$$

  The direction $\supseteq$ holds for sure. So what we really have to show is $\subseteq$, namely
$$g \in \langle r_0, r_1 \rangle \cap \langle r_1, r_2 \rangle \Rightarrow g \in \langle r_1 \rangle \ .$$

Remark. It turns out that Coxeter groups do satisfy the intersection condition. This is tricky to prove. In other words, it is the unstated 'extra' relations that can befoul the intersection condition. Much of one's time in regular polytope theory is spent dealing with this fact.