GROUPS AND SYMMETRY

N. P. STRICKLAND

1. Symmetry groups in $\mathbb{R}^n$

1.1. **General linear groups.** We write M_n or $M_n(\mathbb{R})$ for the set of $n \times n$ matrices over the real numbers. Recall that an $n \times n$ matrix A is *invertible* if there is a matrix B such that $AB = I = BA$. This holds iff $\det(A) \neq 0$, and in that case the matrix B is unique, and we call it A^{-1}.

We write GL_n or $GL_n(\mathbb{R})$ for the set of invertible $n \times n$ matrices over $\mathbb{R}$.

Recall that a *group* is a set G equipped with a binary operation $*$ and an element $e \in G$ such that

- The set G is closed under $*$, in other words $a * b \in G$ whenever $a, b \in G$.
- The operation is associative, in other words $a * (b * c) = (a * b) * c$ whenever $a, b, c \in G$.
- e is a neutral element, in other words $e * a = a = a * e$ for all $a \in G$.
- The operation has inverses: for any $a \in G$ there exists an element $a^{-1} \in G$ with $a * a^{-1} = e = a^{-1} * a$.

For most groups in this course, we will write ab for $a * b$ and 1 for e.

It is easy to check that GL_n is a group under matrix multiplication; it is called the *general linear group*.

1.2. **Orthogonal groups.** Given vectors $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ in $\mathbb{R}^n$, we define

$$\begin{aligned} \langle x, y \rangle &= \sum_{i=1}^{n} x_i y_i \\ \|x\| &= \sqrt{\langle x, x \rangle} = \text{ the length of } x \\ d(x, y) &= \|x - y\| = \text{ the distance from } x \text{ to } y \ . \end{aligned}$$

Proposition 1.1 (The Cauchy-Schwartz inequality)**.** *For any $x, y \in \mathbb{R}^n$ we have $|\langle x, y \rangle| \leq \|x\| \, \|y\|$.*

Proof. (This is included for completeness but is not examinable.)

For any $t \in \mathbb{R}$ we define

$$\begin{aligned} f(t) &= \|x + ty\|^2 \\ &= \langle x + ty, x + ty \rangle \\ &= \langle x, x \rangle + 2t\langle x, y \rangle + t^2 \langle y, y \rangle \\ &= \|x\|^2 + t^2 \|y\|^2 + 2t\langle x, y \rangle. \end{aligned}$$

From the first part of the definition we see that $f(t) \geq 0$ for all t. We now take $t = -\langle x, y \rangle / \|y\|^2$; the geometric interpretation is that in this case $x + ty$ is the projection of x perpendicular to y. Then

$$t^2 \|y\|^2 = \langle x, y \rangle^2 \|y\|^2 / \|y\|^4 = \langle x, y \rangle^2 / \|y\|^2$$

and

$$2t\langle x, y \rangle = -2\langle x, y \rangle^2 / \|y\|^2$$

so

$$f(t) = \|x\|^2 + t^2 \|y\|^2 + 2t\langle x, y \rangle = \|x\|^2 - \langle x, y \rangle^2 / \|y\|^2.$$

Date: February 6, 2020.

Thus, the inequality $f(t) \geq 0$ gives $\|x\|^2 \geq \langle x, y\rangle^2/\|y\|^2$ or equivalently $\|x\| \, \|y\| \geq \langle x, y\rangle$. All this assumes that $y \neq 0$ but the case $y = 0$ is trivial. □

This allows us to define the angle between two nonzero vectors x and y to be the number $\theta \in [0, \pi]$ such that $\langle x, y\rangle = \|x\|\|y\| \cos(\theta)$.

Proposition 1.2 (The triangle inequality)**.** *We have $\|x + y\| \leq \|x\| + \|y\|$, and $d(x, z) \leq d(x, y) + d(y, z)$.*

Proof. Using the Cauchy-Schwartz inequality, we have

$$\begin{aligned}(\|x\| + \|y\|)^2 &= \|x\|^2 + \|y\|^2 + 2\|x\| \, \|y\| \\ &\geq \|x\|^2 + \|y\|^2 + 2\langle x, y\rangle \\ &= \|x + y\|^2.\end{aligned}$$

By taking square roots we get $\|x\| + \|y\| \geq \|x + y\|$, and thus

$$d(x, y) + d(y, z) = \|y - x\| + \|z - y\| \geq \|(y - x) + (z - y)\| = \|z - x\| = d(x, z).$$

□

Next recall that A^T denotes the transpose of A, so the rows of A^T are the columns of A, or in other words $(A^T)_{ij} = A_{ji}$. It is easy to check that

$$\langle x, Ay\rangle = \langle A^T x, y\rangle = \sum_{i,j} x_i A_{ij} y_j.$$

Proposition 1.3. *If $A \in M_n$, then the following conditions are equivalent:*

(a) *A is invertible with $A^{-1} = A^T$.*
(b) *A preserves inner products, or in other words $\langle Ax, Ay\rangle = \langle x, y\rangle$ for all $x, y \in \mathbb{R}^n$.*
(c) *A preserves lengths, or in other words $\|Ax\| = \|x\|$ for all $x \in \mathbb{R}^n$.*
(d) *A preserves distances, or in other words $d(Ax, Ay) = d(x, y)$ for all $x, y \in \mathbb{R}^n$.*

Proof. (a)⇒(b): If $A^T = A^{-1}$ then

$$\langle Ax, Ay\rangle = \langle A^T Ax, y\rangle = \langle A^{-1} Ax, y\rangle = \langle x, y\rangle.$$

(b)⇒(c)⇒(d): this is trivial, as lengths are defined in terms of inner products, and distances are defined in terms of lengths.

(d)⇒(c): If A preserves distances then $\|Ax\| = d(Ax, A0) = d(x, 0) = \|x\|$.

(c)⇒(b): Note that

$$\|x + y\|^2 = \langle x + y, x + y\rangle = \|x\|^2 + \|y\|^2 + 2\langle x, y\rangle,$$

so

$$\langle x, y\rangle = (\|x + y\|^2 - \|x\|^2 - \|y\|^2)/2.$$

Thus, if A preserves lengths we have

$$\begin{aligned}\langle Ax, Ay\rangle &= (\|Ax + Ay\|^2 - \|Ax\|^2 - \|Ay\|^2)/2 \\ &= (\|A(x + y)\|^2 - \|Ax\|^2 - \|Ay\|^2)/2 \\ &= (\|x + y\|^2 - \|x\|^2 - \|y\|^2)/2 \\ &= \langle x, y\rangle.\end{aligned}$$

(b)⇒(a): Suppose that $\langle Ax, Ay\rangle = \langle x, y\rangle$ for all x, y. We also have $\langle Ax, Ay\rangle = \langle x, A^T Ay\rangle$, so we deduce that $\langle x, y - A^T Ay\rangle = 0$. This means that $y - A^T Ay$ is orthogonal to every vector in $\mathbb{R}^n$. In particular, it is orthogonal to itself, so it must be zero, so $y = A^T Ay$ for all y. This shows that $A^T A = I$, so A^T is an inverse for A. (Here we are using the fact that if A and B are square matrices of the same size and $BA = I$ then $AB = I$ also. Why is this false for non-square matrices?) □

Definition 1.4. A matrix A is *orthogonal* if it satisfies the equivalent conditions in the Proposition. We write O_n for the set of $n \times n$ orthogonal matrices, and call this the *orthogonal group*.

Proposition 1.5. *O_n is a subgroup of GL_n.*

Proof. We need to check that (1) the identity matrix is in O_n, (2) if $A \in O_n$ then $A^{-1} \in O_n$ and (3) if $A, B \in O_n$ then $AB \in O_n$. Condition (1) is clear, because $I^T = I = I^{-1}$. If $A \in O_n$ then $A^T A = I$ and $A^{TT} = A$ so if we put $C = A^T$ we see that $CC^T = I$, so $C \in O_n$. On the other hand, we also have $C = A^{-1}$ so $A^{-1} \in O_n$ as required. Finally, if $A, B \in O_n$ then $(AB)^T = B^T A^T$ and $BB^T = I$ and $AA^T = I$, so $AB(AB)^T = ABB^T A^T = AA^T = I$. Thus $AB \in O_n$. □

1.3. **Determinants.** Recall that the *determinant* of an $n \times n$ matrix A is given by the formula

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} A_{i,\sigma(i)}.$$

In other words, for each permutation σ of $\{1, \dots, n\}$ we form the product

$$A_{1,\sigma(1)} A_{2,\sigma(2)} \dots A_{n,\sigma(n)},$$

we multiply by the signature of σ and then add all these terms up to get the determinant. For example, when $n = 2$ we just have the identity permutation ι and the transposition $\tau = (1\ 2)$, and so we have the familiar formula

$$\det \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} = \operatorname{sgn}(\iota) A_{1,\iota(1)} A_{2,\iota(2)} + \operatorname{sgn}(\tau) A_{1,\tau(1)} A_{2,\tau(2)} = A_{11}A_{22} - A_{12}A_{21}.$$

Much more important than the definition is the following list of properties:

(a) $\det(I) = 1$
(b) $\det(AB) = \det(A)\det(B)$
(c) $\det(A^T) = \det(A)$
(d) If we multiply a single row in A by a number t to get a new matrix A', then $\det(A') = t\det(A)$. The same thing works for columns instead of rows.
(e) If we add a multiple of one row in A to another row to get a new matrix A', then $\det(A') = \det(A)$.
(f) $\det(tA) = t^n \det(A)$ for $t \in \mathbb{R}$ (for example $\det \begin{pmatrix} ta & tb \\ tc & td \end{pmatrix} = t^2 ad - t^2 bc = t^2 \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}$).

If A is invertible then $\det(A)\det(A^{-1}) = \det(I) = 1$, so $\det(A) \neq 0$. Thus det can be thought of as a function from $GL_n = \{\text{invertible } n \times n \text{ matrices}\}$ to the set $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$. Let D_t be the matrix obtained from I by multiplying the first row by t; for example, when $n = 4$ we have

$$D_t = \left(\begin{array}{c|ccc} t & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

We then have $\det(D_t) = t$; this shows that the function $\det\colon GL_n \to \mathbb{R}^\times$ is surjective. Moreover, $\mathbb{R}^\times$ is a group under multiplication, and properties (a) and (b) can be restated as follows:

Proposition 1.6. *The determinant gives a surjective homomorphism* $\det\colon GL_n \to \mathbb{R}^\times$. □

We next recall the First Isomorphism Theorem:

Theorem 1.7. *If* $\phi\colon G \to H$ *is a surjective homomorphism of groups and* $N = \{g \in G \mid \phi(g) = 1\}$ *is the kernel of* ϕ*, then:*

(a) *N is a normal subgroup of G; in other words, it contains 1, is closed under multiplication and inversion, and satisfies $gNg^{-1} = N$ for all $g \in G$.*
(b) *It follows that there is a quotient group G/N. The elements of G/N are the cosets of N. For each coset C we can choose $g \in G$ such that $C = gN$, but there will usually be many choices for g.*
(c) *There is a unique function $\overline{\phi}\colon G/N \to H$ with $\overline{\phi}(gN) = \phi(g)$ for all $g \in G$.*
(d) *The function $\overline{\phi}$ is actually an isomorphism of groups.* □

Definition 1.8. We write

$$SL_n = \ker(\det\colon GL_n \to \mathbb{R}^\times) = \{n \times n \text{ matrices } A \text{ such that } \det(A) = 1\},$$

and call this the *special linear group.*

The First Isomorphism Theorem implies:

Proposition 1.9. *SL_n is a normal subgroup of GL_n, and there is a natural isomorphism*

$$\overline{\det}\colon GL_n/SL_n \to \mathbb{R}^\times. \quad \square$$

1.4. **Orthogonal determinants.**

Lemma 1.10. *If $A \in O_n$ then $\det(A) \in \{1, -1\} = \{\pm 1\}$.*

Proof. $\det(A)^2 = \det(A)\det(A^T) = \det(AA^T) = \det(I) = 1.$ $\square$

Clearly $\{\pm 1\}$ is a subgroup of $\mathbb{R}^\times$, and det gives a homomorphism from O_n to $\{\pm 1\}$. Clearly $D_{-1}^T D_{-1} = D_{-1}^2 = I$, so $D_{-1} \in O_n$, and $\det(D_{-1}) = -1$, so our homomorphism $\det\colon O_n \to \{\pm 1\}$ is surjective.

Definition 1.11. We write

$$SO_n = \ker(\det\colon O_n \to \{\pm 1\}) = \{n \times n \text{ orthogonal matrices } A \text{ such that } \det(A) = 1\},$$

and call this the *special orthogonal group*.

The First Isomorphism Theorem gives:

Proposition 1.12. *SO_n is a normal subgroup of O_n, and there is a natural isomorphism*

$$\overline{\det}\colon O_n/SO_n \to \{\pm 1\}.$$

1.5. **One dimension.** A 1×1 matrix is just a number. Thus $GL_1 = \mathbb{R}^\times$, and $O_1 = \{\pm 1\}$. The determinant map is just the identity, so $SL_1 = SO_1 = \{1\}$, the trivial group.

1.6. **Two dimensions.** Given an angle θ, we write $c = \cos(\theta)$ and $s = \sin(\theta)$ (so $s^2 + c^2 = 1$) and define matrices as follows:

$$R_\theta = \begin{pmatrix} c & -s \\ s & c \end{pmatrix} \qquad S_\theta = \begin{pmatrix} c & s \\ s & -c \end{pmatrix}.$$

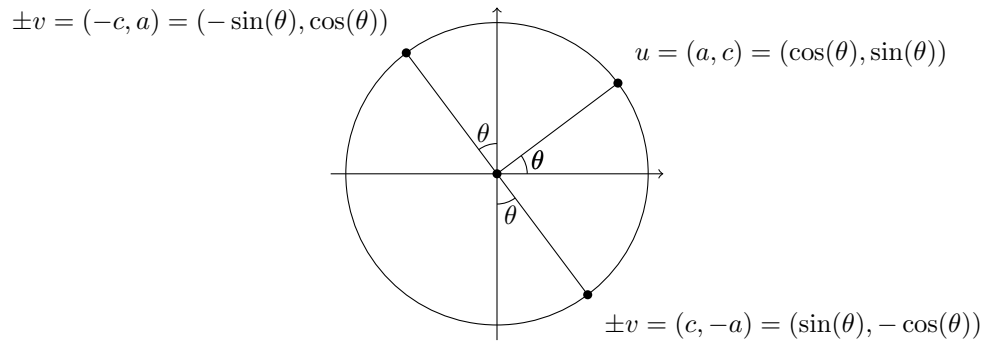
It is easy to see that these are orthogonal, and that $\det(R_\theta) = 1$ and $\det(S_\theta) = -1$. Thus $R_\theta \in SO_2$ and $S_\theta \in O_2 \setminus SO_2$.

Theorem 1.13. *Any matrix $A \in SO_2$ has the form R_θ for some θ. Any matrix $A \in O_2 \setminus SO_2$ has the form S_θ for some θ.*

Proof. Suppose $A \in O_2$. We have $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ for some a, b, c, d. As A is orthogonal we have $I = A^T A$, so

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{pmatrix},$$

so $a^2 + c^2 = b^2 + d^2 = 1$ and $ab + cd = 0$. In other words, the vectors $u = (a, c)$ and $v = (b, d)$ have length one and are orthogonal to each other. As u is a unit vector, we have $u = (\cos(\theta), \sin(\theta))$ for some θ, so $a = \cos(\theta)$ and $c = \sin(\theta)$. It is geometrically clear (see the diagram below) that the only unit vectors orthogonal to u are $(-c, a) = (-\sin(\theta), \cos(\theta))$ and $(c, -a) = (\sin(\theta), \cos(\theta))$. If $v = (-c, a)$ we find that $A = R_\theta$, and if $v = (c, -a)$ we find that $A = S_\theta$. By equating determinants, we see that the first case must occur if $A \in SO_2$, and the second case must occur if $A \in O_2 \setminus SO_2$.



□

In $\mathbb{R}^2$ it is often convenient to use polar coordinates. We will write $[r, \phi]$ for the point at distance r from the origin and angle ϕ to the x axis, so

$$[r, \phi] = (r\cos(\phi), r\sin(\phi)).$$

Note that $[r, \phi] = [r', \phi']$ iff $r = r' = 0$ or ($r = r' \neq 0$ and $\phi - \phi'$ is an integer multiple of 2π).

Proposition 1.14. *We have $R_\theta.[r, \phi] = [r, \theta + \phi]$, so R_θ represents an anticlockwise rotation through an angle θ.*

Proof.

$$\begin{aligned} R_\theta.[r, \phi] &= \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} r\cos(\phi) \\ r\sin(\phi) \end{pmatrix} \\ &= r \begin{pmatrix} \cos(\theta)\cos(\phi) - \sin(\theta)\sin(\phi) \\ \sin(\theta)\cos(\phi) + \cos(\theta)\sin(\phi) \end{pmatrix} \qquad = \begin{pmatrix} r\cos(\theta + \phi) \\ r\sin(\theta + \phi) \end{pmatrix} = [r, \theta + \phi]. \end{aligned}$$

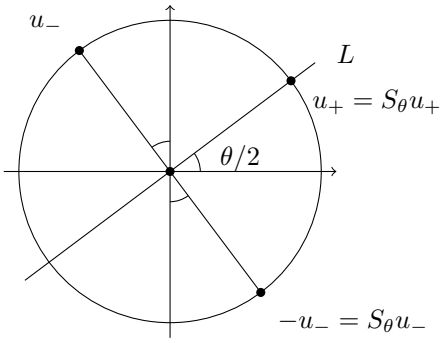
□

We also want to characterise S_θ geometrically. Firstly, a very similar calculation shows that $S_\theta.[r, \phi] = [r, \theta - \phi]$. Now define $u_+ = [1, \theta/2]$ and $u_- = [1, (\theta + \pi)/2]$, so that u_+ and u_- are unit vectors and are orthogonal to each other. Note also that $-[r, \phi] = [r, \phi - \pi]$, so $-u_- = [1, (\theta - \pi)/2]$. We have

$$\begin{aligned} S_\theta.u_+ &= [1, \theta - \theta/2] = [1, \theta/2] = u_+ \\ S_\theta.u_- &= [1, \theta - \theta/2 - \pi/2] = [1, (\theta - \pi)/2] = -u_-. \end{aligned}$$

Thus u_+ and u_- are eigenvectors of S_θ with eigenvalues $+1$ and -1 respectively. This means that S_θ represents reflection across the line through 0 and u_+. We summarise our conclusions as follows:

Proposition 1.15. *We have $S_\theta.[r, \phi] = [r, \theta - \phi]$, and S_θ represents reflection across a line L through 0 at angle $\theta/2$ to the x-axis.* □



By working in polar coordinates, it is now easy to check the following facts:

$$\begin{aligned} R_\theta &= R_\phi && \text{iff } \theta - \phi \in 2\pi\mathbb{Z} \\ S_\theta &= S_\phi && \text{iff } \theta - \phi \in 2\pi\mathbb{Z} \\ R_\theta R_\phi &= R_{\theta+\phi} \\ R_\theta S_\phi &= S_{\theta+\phi} \\ S_\theta R_\phi &= S_{\theta-\phi} \\ S_\theta S_\phi &= R_{\theta-\phi} \\ R_\theta^{-1} &= R_{-\theta} \\ S_\theta^{-1} &= S_\theta \\ R_\theta S_\phi R_\theta^{-1} &= S_{\phi+2\theta}. \end{aligned}$$

In particular, we have $R_\theta R_\phi = R_\phi R_\theta$, so the group SO_2 is Abelian.

We also have $S_\theta S_\theta = R_{\theta-\theta} = R_0 = I$, so all reflections have order 2. A rotation R_θ has order dividing m iff $m\theta$ is an integer multiple of 2π, iff $\theta = 2\pi r/m \pmod{2\pi\mathbb{Z}}$ for some $r \in \{0, 1, \dots, m-1\}$. It has order exactly m iff $(r, m) = 1$. Most rotations have infinite order.

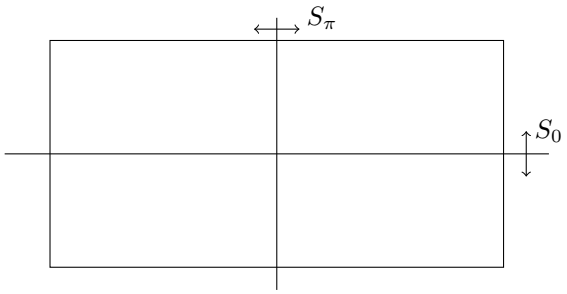
1.7. **Symmetries of geometric objects.** Let X be a subset of $\mathbb{R}^n$. For any $A \in O_n$ we put $AX = \{Ax \mid x \in X\}$, the image of X under A. The *symmetry group* of X is

$$\mathrm{Symm}(X) = \{A \in O_n \mid AX = X\}.$$

The *direct symmetry group* is

$$\mathrm{Dir}(X) = \{A \in SO_n \mid AX = X\} = \mathrm{Symm}(X) \cap SO_n.$$

Example 1.16. Let X be a rectangle as shown below.



It is clearly invariant under the reflections S_0 (across the x-axis) and S_π (across the y-axis), and also under a half-turn (which is R_π). We have $S_0 S_\pi = S_\pi S_0 = R_\pi = R_{-\pi}$ and $R_0 = I$. The symmetry groups are

$$\mathrm{Symm}(X) = \{I, S_0, S_\pi, R_\pi\}$$
$$\mathrm{Dir}(X) = \{I, R_\pi\}.$$

Now suppose that A is *not* a symmetry of X. Then AX is different from X, but it has the same shape and thus is "just as symmetrical" as X. However, it it not true (as one might naively think) that $\mathrm{Symm}(AX) = \mathrm{Symm}(X)$; instead, $\mathrm{Symm}(AX)$ is conjugate to $\mathrm{Symm}(X)$. The slogan is that "conjugacy is doing the same thing somewhere else".

Proposition 1.17. *For any $X \subseteq \mathbb{R}^n$ and $A \in O_n$ we have* $\mathrm{Symm}(AX) = A\,\mathrm{Symm}(X)A^{-1}$ *and* $\mathrm{Dir}(AX) = A\,\mathrm{Dir}(X)A^{-1}$.

Proof. If $B \in \mathrm{Symm}(X)$ then $BX = X$ so $(ABA^{-1})(AX) = ABX = AX$, which shows that $ABA^{-1} \in \mathrm{Symm}(AX)$. Thus $A\,\mathrm{Symm}(X)A^{-1} \subseteq \mathrm{Symm}(AX)$. Conversely, suppose that $C \in \mathrm{Symm}(AX)$. If we put $B = A^{-1}CA$, then a similar argument shows that $B \in \mathrm{Symm}(X)$. Thus, the matrix $C = ABA^{-1}$ lies in $A\,\mathrm{Symm}(X)A^{-1}$, proving that $\mathrm{Symm}(AX) \subseteq A\,\mathrm{Symm}(X)A^{-1}$ as required.

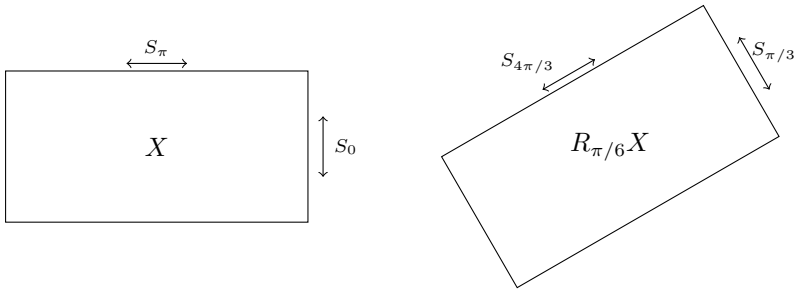
The argument for $\mathrm{Dir}(X)$ is the same. It works even if $A \notin SO_n$, because

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A)^{-1} = \det(B),$$

so B lies in SO_n iff ABA^{-1} lies in SO_n. □

For another example of this sort of phenomenon let L be a line through the origin, and let S_L be the reflection across L. If L has angle ϕ to the x-axis, then $S_L = S_{2\phi}$. The line $R_\theta L$ has angle $\theta + \phi$ to the x-axis, so $S_{R_\theta L} = S_{2(\theta+\phi)}$. On the other hand, from our formulae for compositions of reflections and rotations, we see that $R_\theta S_{2\phi} R_\theta^{-1} = S_{2\phi+2\theta}$. In summary, we have:

Proposition 1.18. *For any rotation $R \in SO_2$ and any line L in $\mathbb{R}^2$ we have $RS_LR^{-1} = S_{RL}$.* □



Example 1.19.
We can see directly that

$$\begin{aligned}\mathrm{Symm}(X) &= \{I, S_0, S_\pi, R_\pi\}\\ \mathrm{Symm}(R_{\pi/6}X) &= \{I, S_{\pi/3}, S_{4\pi/3}, R_\pi\}\end{aligned}$$

We also have

$$\begin{aligned}R_{\pi/6} I R_{\pi/6}^{-1} &= I\\ R_{\pi/6} S_0 R_{\pi/6}^{-1} &= S_{\pi/3}\\ R_{\pi/6} S_\pi R_{\pi/6}^{-1} &= S_{4\pi/3}\\ R_{\pi/6} R_\pi R_{\pi/6}^{-1} &= R_\pi.\end{aligned}$$

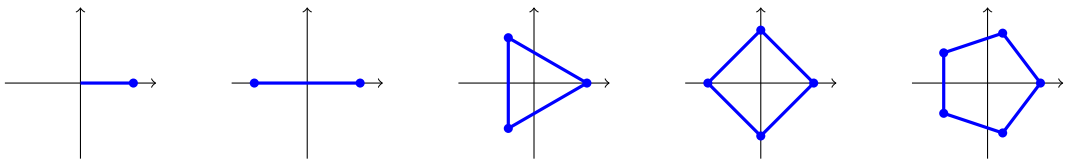
This shows that $\mathrm{Symm}(R_{\pi/6}X) = R_{\pi/6}\,\mathrm{Symm}(X)R_{\pi/6}^{-1}$, illustrating Proposition 1.17. Also, if we let L denote the long axis of X we see that $S_0 = S_L$ and $S_{\pi/3}$ is the reflection in the long axis of $R_{\pi/6}X$, which is $R_{\pi/6}L$. This illustrates Proposition 1.18.

2. Polygons

2.1. **Cyclic and dihedral groups.** Fix an integer $n > 0$. For $k = 0, \dots, n-1$ we put

$$v_k = [1, 2\pi k/n] = (\cos(2\pi k/n), \sin(2\pi k/n)).$$

We then let X_n be the regular n-gon with vertices $v_0, \dots, v_{n-1}$. In the case $n = 1$ this is to be interpreted as the line segment from $(0,0)$ to $v_0 = (1,0)$.



X_1 X_2 X_3 X_4 X_5

We also define

$$\begin{aligned}C_n &= \mathrm{Dir}(X_n)\\ D_n &= \mathrm{Symm}(X_n)\\ R &= R_{2\pi/n} = \text{ } 1/n\text{-turn around the origin}\\ S &= S_0 = \text{ reflection across the } x\text{-axis .}\end{aligned}$$

We call C_n the *cyclic group*, and D_n the *dihedral group*.

Theorem 2.1. *We have*

$$\begin{aligned}C_n &= \{R^i \mid 0 \le i < n\}\\ D_n &= \{R^i \mid 0 \le i < n\} \cup \{R^i S \mid 0 \le i < n\}.\end{aligned}$$

Proof. First, it is clear that $R \in C_n$ and $S \in D_n$, so $C_n \supseteq \{R^i \mid 0 \leq i < n\}$ and $D_n \supseteq \{R^i \mid 0 \leq i < n\} \cup \{R^i S \mid 0 \leq i < n\}$. Suppose that $A \in C_n$. Then $Av_0 \in RX_n$ and $\|Av_0\| = \|v_0\| = 1$. However, it is easy to see that the only vectors in X_n of length 1 are the vertices, so $Av_0 = v_i$ for some i with $0 \leq i < n$. This means that the matrix $A' := R^{-i}A$ satisfies $A'v_0 = v_0$. Also, A' is a rotation, and the only way a rotation of the plane can have a nonzero fixed point is if it is the identity. Thus $A' = I$, so $A = R^i$. Thus $C_n = \{A^i \mid 0 \leq i < n\}$ as claimed.

Now suppose that $B \in D_n$. If $B \in C_n$ then $B = R^i$ for some i by the above. If $B \notin C_n$ then $\det(B) = -1$, so $BS \in D_n$ and $\det(BS) = \det(B)\det(S) = 1$, so $BS = R^i$ for some i. This means that $B = BSS = R^i S$, which proves the claim about D_n. □

Remark 2.2. Because SO_n is normal in O_n, we see that C_n is normal in D_n. It is easy to see that $D_n/C_n \simeq \{\pm 1\}$.

2.2. **The classification of subgroups.**

Proposition 2.3. *Let G be a finite subgroup of SO_2. Then $G = C_n$ for some n.*

Proof. Let θ be the smallest angle in the range $(0, 2\pi]$ such that $R_\theta \in G$. I claim that $\theta = 2\pi/n$ for some n, and that $G = C_n$. To see this, let ϕ be any angle such that $\phi \geq 0$ and $R_\phi \in G$. Let k be the largest integer such that $k\theta \leq \phi$ and put $\psi = \phi - k\theta$. We then have $0 \leq \psi < \theta \leq 2\pi$, and $R_\psi = R_\phi R_\theta^{-k} \in G$. If ψ were in the range $(0, 2\pi]$, this would contradict our definition of θ, so we must have $\psi = 0$. Thus $\phi = k\theta$ and $R_\phi = R_\theta^k$. This shows that the elements of G are precisely the powers of R_θ.

In particular, we have $R_{2\pi} = I \in G$, so we can apply the above argument with $\phi = 2\pi$ and deduce that $2\pi = n\theta$ for some $n > 0$, so $\theta = 2\pi/n$. Thus G consists of the powers of $R_{2\pi/n}$, in other words $G = C_n$. □

Theorem 2.4. *Let G be a finite subgroup of O_2. Then either $G = C_n = \mathrm{Dir}(X_n)$ for some n, or $G = R_\theta D_n R_\theta^{-1} = \mathrm{Symm}(R_\theta X_n)$ for some n and θ.*

Proof. Put $H = G \cap SO_2$; the Proposition tells us that $H = C_n$ for some n. If $G \leq SO_2$ then $G = H = C_n$. Otherwise G contains some reflection, say $S_{2\theta} \in G$. If $A \in G$ then either

(a) $\det(A) = 1$, so $A \in H$ and $A = R_{2\pi/n}^k$ for some k; or
(b) $\det(A) = -1$ so $AS_{2\theta} \in G$ and $\det(AS_{2\theta}) = 1$ so $AS_{2\theta} = R_{2\pi/n}^k$ for some k so $A = R_{2\pi/n}^k S_{2\theta}$.

Next, note that $R_\theta^{-1} R_{2\pi/n}^k R_\theta = R_{2\pi/n}^k$ and $R_\theta^{-1} S_{2\theta} R_\theta = S_0$. It follows that the group $G' := R_\theta^{-1} G R_\theta$ consists of the elements $R_{2\pi/n}^k$ and $R_{2\pi/n}^k S_0$, or in other words $G' = D_n$. Thus $G = R_\theta G' R_\theta^{-1} = R_\theta D_n R_\theta^{-1}$, as required. □

3. Affine isometries

Definition 3.1. An *isometry* of $\mathbb{R}^n$ is a function $f\colon \mathbb{R}^n \to \mathbb{R}^n$ of the form $f(x) = Ax + a$ for some orthogonal matrix $A \in O_n$ and some vector $a \in \mathbb{R}^n$. We write Isom_n for the set of all such functions.

Remark 3.2. If we have an isometry $f(x) = Ax + a$ as above, then $d(f(x), f(y)) = d(x, y)$ for all x and y in $\mathbb{R}^n$, or in other words, f preserves distances. To see this, note that

$$d(f(x), f(y)) = \|(Ax + a) - (Ay + a)\| = \|A(x - y)\| = \|x - y\| = d(x, y).$$

(At the third step we used the fact that A is an orthogonal matrix, so $\|Az\| = \|z\|$ for any vector $z \in \mathbb{R}^n$.)

Remark 3.3. Let $f\colon \mathbb{R}^n \to \mathbb{R}^n$ be any function that preserves distances. It can be shown that there is a matrix $A \in O_n$ and a vector $a \in \mathbb{R}^n$ such that $f(x) = Ax + a$ for all x, so $f \in \mathrm{Isom}_n$. (The proof takes about a page and a half, but we will not give it here.) This means that Definition 3.1 is compatible with the general definition of isometries for metric spaces.

Remark 3.4. Suppose we have isometries $f(x) = Ax + a$ and $g(x) = Bx + b$. Then

$$f(g(x)) = (AB)x + (Ab + a)$$
$$f^{-1}(x) = A^{-1}x + (-A^{-1}a).$$

We have $AB \in O_n$ and $Ab+a \in \mathbb{R}^n$ so $f \circ g \in \mathrm{Isom}_n$. Similarly $A^{-1} \in O_n$ and $-A^{-1}a \in \mathbb{R}^n$ so $f^{-1} \in \mathrm{Isom}_n$. This shows that Isom_n is a group under composition. We will usually write fg instead of $f \circ g$, and write 1 for the identity map.

We will not distinguish between a matrix $A \in O_n$ and the corresponding isometry $f(x) = Ax$. We thus think of O_n as a subgroup of Isom_n.

For any $a \in \mathbb{R}^n$ we have an isometry T_a defined by $T_a(x) = x + a$; this is called a *translation*. We clearly have $T_a T_b = T_{a+b}$ and $T_a^{-1} = T_{-a}$. It follows that the translations form an abelian subgroup $\mathrm{Trans}_n \leq \mathrm{Isom}_n$. Using the correspondence $T_a \leftrightarrow a$ we can identify Trans_n with $\mathbb{R}^n$.

3.1. **The homomorphism ψ.**

Definition 3.5. Given an isometry $f(x) = Ax + a$, we define $\psi(f) = A \in O_n$ and $\det(f) = \det(A) = \det(\psi(f)) \in \{1, -1\}$. This gives functions $\psi\colon \mathrm{Isom}_n \to O_n$ and $\det\colon \mathrm{Isom}_n \to \{1, -1\}$.

Proposition 3.6. *The map ψ is a surjective homomorphism with kernel Trans_n, and thus it induces an isomorphism $\mathrm{Isom}_n / \mathrm{Trans}_n \simeq O_n$. Moreover, $\det\colon \mathrm{Isom}_n \to \{\pm 1\}$ is also a homomorphism.*

Proof. First suppose we have $f(x) = Ax + a$ and $g(x) = Bx + b$. Then

$$fg(x) = f(Bx + b) = A(Bx + b) + a = ABx + (Ab + a),$$

which shows that $\psi(fg) = AB = \psi(f)\psi(g)$. This shows that ψ is a homomorphism, and it follows that $\det\colon \mathrm{Isom}_n \to \{\pm 1\}$ is also a homomorphism. For any $A \in O_n$ we can define an isometry f by $f(x) = Ax$ and then $\psi(f) = A$, which shows that ψ is surjective. We have $\psi(f) = I$ iff $f(x) = x + a$ for all x, iff f is a translation, so $\ker(\psi)$ is the translation subgroup Trans_n. It now follows from the First Isomorphism Theorem that $\mathrm{Isom}_n / \mathrm{Trans}_n \simeq O_n$. □

Proposition 3.7. *For any $f \in \mathrm{Isom}_n$ and $b \in \mathbb{R}^n$ we have $fT_b f^{-1} = T_{\psi(f)a}$.*

(This is meaningful because $\psi(f) \in O_n$ is a matrix and a is a vector so $\psi(f)a$ is another vector, so we have a translation function $T_{\psi(f)a}$.)

Proof. We can write $f(x) = Ax + a$, where $A = \psi(f)$. We then have

$$fT_b(x) = f(x + b) = Ax + Ab + a = f(x) + Ab = T_{Ab} f(x).$$

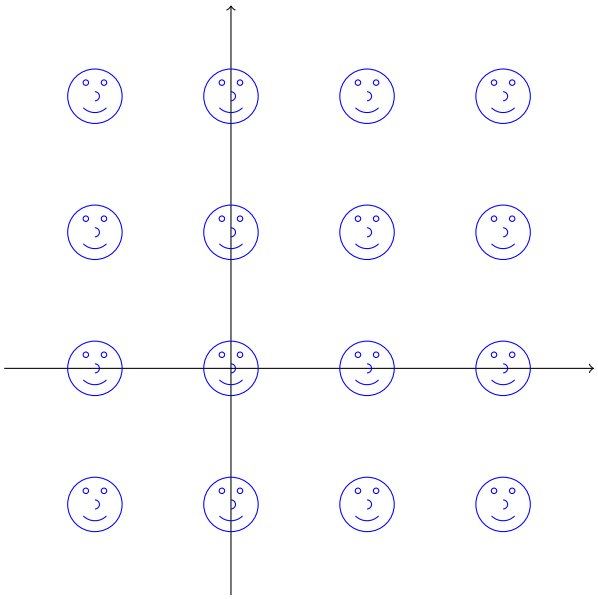
Thus, $fT_b = T_{Ab} f$, and we can multiply by f^{-1} on the right to get $fT_b f^{-1} = T_{Ab} = T_{\psi(f)b}$. □

Definition 3.8. For any subset $X \subseteq \mathbb{R}^n$, we put

$$\mathrm{Isom}(X) = \{f \in \mathrm{Isom}_n \mid f(X) = X\},$$

and call this the *isometry group* of X.

Example 3.9. Let X be the subset of $\mathbb{R}^2$ illustrated below. It extends infinitely in all directions, and the distance between adjacent faces is one unit.



If we shift X by n units to the right and m units up, we just get X again (assuming that n and m are integers). In other words, $T_{(n,m)}X = X$, so $T_{(n,m)} \in \mathrm{Isom}(X)$. In fact, one can check that these are the only symmetries, so $\mathrm{Isom}(X) = \{T_{(n,m)} \mid (n,m) \in \mathbb{Z}^2\}$.

We conclude this section by giving a simple criterion for when an isometry is the identity.

Definition 3.10. A list $u_0, \dots, u_n$ of $n+1$ points in $\mathbb{R}^n$ is in *general position* if the vectors $u_1 - u_0, \dots, u_n - u_0$ form a basis of $\mathbb{R}^n$.

Proposition 3.11. *If $u_0, \dots, u_n$ are in general position, $f \in \mathrm{Isom}_n$ and $f(u_i) = u_i$ for all i, then $f = 1$.*

Proof. We have $f(x) = Ax + b$ for some A, b. It follows that

$$A(u_i - u_0) = (Au_i + b) - (Au_0 + b) = f(u_i) - f(u_0) = u_i - u_0$$

for all i. As the vectors $u_i - u_0$ form a basis, we deduce that $A = I$, so $f(x) = x + b$ for all x. In particular, $u_0 = f(u_0) = u_0 + b$, so $b = 0$. Thus $f(x) = x$ for all x as claimed. □

4. Plane isometries

We next define some special types of isometries of $\mathbb{R}^2$.

(1) For any $a \in \mathbb{R}^2$ and any angle θ, we put $R_{\theta,a} = T_a R_\theta T_{-a}$, so that

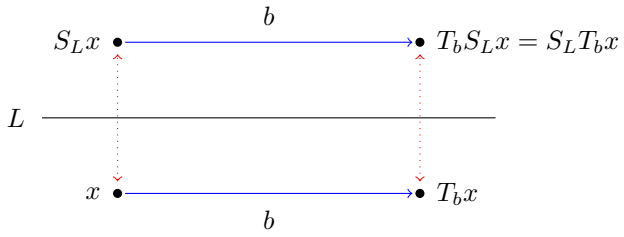
$$R_{\theta,a}(x) = a + R_\theta(x - a) = R_\theta x + (1 - R_\theta)a.$$

Note that $R_{\theta,a}(a + x) = a + R_\theta x$, which means that $R_{\theta,a}$ is the rotation through angle θ around a. If θ is not a multiple of 2π then for all $x \neq 0$ we have $R_\theta x \neq 0$; it follows that a is the unique fixed point of $R_{\theta,a}$. Note also that $\psi(R_{\theta,a}) = R_\theta$.

(2) For any line $L < \mathbb{R}^2$ (not necessarily passing through the origin) we let S_L be the reflection across L. If L has angle $\theta/2$ to the x-axis and $a \in L$ one checks that $S_L = T_a S_\theta T_{-a}$. We also have $\psi(S_L) = S_\alpha$, where α is the angle between L and the x-axis.

(3) For any line $L < \mathbb{R}^2$ and any vector b that is parallel to L, we define $G_{L,b} = T_b S_L$. It is not hard to check geometrically that $G_{L,b} = S_L T_b$ also, and it follows that

$$G_{L,b}^2 = (T_b S_L)(S_L T_b) = T_b^2 = T_{2b}.$$



Clearly $G_{L,0} = S_L$. Maps of the form $G_{L,b}$ with $b \neq 0$ are called *glide-reflections*. We have $\psi(G_{L,b}) = S_\alpha$, where α is the angle between L and the x-axis.

Proposition 4.1. *For any $f \in \mathrm{Isom}_2$, precisely one of the following holds:*

(a) $f = 1$
(b) $f = T_a$ *for some* $a \in \mathbb{R}^2 \setminus \{0\}$
(c) $f = R_{\theta,a}$ *for some* $a \in \mathbb{R}^2$ *and* $\theta \in (0, 2\pi)$
(d) $f = S_L$ *for some line* $L < \mathbb{R}^2$
(e) $f = G_{L,b}$ *for some* L *and some nonzero vector* b *parallel to* L.

Proof. We know that there exists a matrix $A \in O_2$ and a vector b such that $f(x) = Ax + b$ for all x. If $A = I$ then we are in case (a) (if $b = 0$) or case (b) (if $b \neq 0$). We may thus assume that $A \neq I$.

If A is a rotation we have $A = R_\theta$ for some $\theta \in (0, 2\pi)$. As A is a nontrivial rotation, for all x we have $x \neq Ax$ so $(I - A)x \neq 0$. Thus, the kernel of $I - A$ is zero, so $I - A$ is invertible. Put $a = (I - A)^{-1}b$, so that $b = a - Aa$. Then

$$R_{\theta,a}x = T_aAT_{-a}x = A(x - a) + a = Ax + a - Aa = Ax + b = f(x),$$

so $f = R_{\theta,a}$.

Now suppose instead that A is a reflection, say $A = S_\theta$. As before we put $u_+ = [1, \theta/2]$ and $u_- = [1, (\theta + \pi)/2]$, so u_+ and u_- are unit vectors and are orthogonal to each other. We can write any vector x in the form $x_+ + x_-$, where $x_\pm$ is a multiple of $u_\pm$, and then $Ax = x_+ - x_-$. It follows that

$$f(x) = Ax + b = x_+ - x_- + b_+ + b_- = (b_+ + x_+) + (b_- - x_-).$$

Now let L be the line through $b_-/2$ at angle $\theta/2$ to the x-axis. We can write any vector x as $(x_+ + \frac{1}{2}b_-) + (x_- - \frac{1}{2}b_-)$, where $(x_+ + \frac{1}{2}b_-) \in L$ and $(x_- - \frac{1}{2}b_-)$ is orthogonal to L. It follows that

$$S_Lx = (x_+ + \tfrac{1}{2}b_-) - (x_- - \tfrac{1}{2}b_-) = x_+ + b_- - x_-,$$

and thus that

$$G_{L,b_+}x = b_+ + x_+ + b_- - x_- = f(x).$$

Thus, $f = G_{L,b_+}$, so f is a reflection (if $b_+ = 0$) or a glide-reflection (if $b_+ \neq 0$). □

Remark 4.2. Suppose we have an isometry f, and we want to know where it falls in the above clasification. One can check using the above proof that the following method will work.

(a) Find the matrix $A = \psi(f) \in O_2$.
(b) If A is the identity, then $f = T_u$ for some u. To find u, let x be any point for which one can easily find $f(x)$, and then $u = f(x) - x$.
(c) Now suppose that $\psi(f) = R_\theta$ for some angle $\theta \in (0, 2\pi)$. Then there is a unique point a such that $f(a) = a$, and it works out that $f = R_{\theta,a}$.
(d) Suppose instead that $\psi(f) = S_\theta$ for some θ. Then we choose a point x for which we can easily calculate $f(f(x))$, and put $u = (f(f(x)) - x)/2$. We then put $L = \{x \mid f(x) = x + u\}$. It works out that L is always a line parallel to u, and that $f = G_{L,u}$ (if $u \neq 0$) or $f = S_L$ (if $u = 0$).

4.1. **Subgroups with no translations.**

Theorem 4.3. *Let H be a subgroup of* Isom_2*, and suppose that H contains no translations (other than the trivial translation $T_0 = 1$). Then there is a point $a \in \mathbb{R}^2$ such that $f(a) = a$ for all $f \in H$, and thus $H \leq T_aO_2T_a^{-1}$.*

This theorem implies a classification of finite subgroups of Isom_2, as will be explained in Corollary 4.5. The proof relies on the following lemma.

Lemma 4.4. (a) *$(R_{a,\theta}S_L)^2 = T_c$, where $c = (1 - R_\theta)(a - S_L(a))$.*

(b) *$R_{a,\theta}R_{b,\phi}R_{a,\theta}^{-1}R_{b,\phi}^{-1} = T_d$, where $d = (1 - R_\phi)(1 - R_\theta)(a - b)$.*

(c) *If K and L are parallel then there is a vector u perpendicular to K and L such that $L = K + u$, and $S_L S_K = T_{2u}$.*

(d) *If K and L are not parallel then they meet at a unique point a, and there is a unique angle $\theta \in [0, \pi)$ such that $L = R_{a,\theta}K$, and $S_L S_K = R_{2\theta,a}$.*

We will first prove the theorem using the lemma, then we will prove the lemma.

Proof of Theorem 4.3. I first claim that H contains no glide-reflections. Indeed, if $G_{L,b} \in H$ then $G_{L,b}^2 \in H$ but $G_{L,b}^2 = T_{2b}$ and $2b \neq 0$, contrary to our assumption about H. Thus every element of H is either the identity, a nontrivial rotation, or a reflection.

Now suppose that H contains a nontrivial rotation $R_{a,\theta}$. Because this is nontrivial we have $R_\theta(x) \neq x$ for all x, so $(1 - R_\theta)(x) \neq 0$, so $1 - R_\theta$ is invertible. I claim that $f(a) = a$ for all $f \in H$. This is clear if $f = 1$. If f is a nontrivial rotation, say $f = R_{b,\phi}$, then we note that the element $g = R_{a,\theta}R_{b,\phi}R_{a,\theta}^{-1}R_{b,\phi}^{-1}$ also lies in H. Part (b) of the lemma tells us that $g = T_d$, where $d = (1 - R_\phi)(1 - R_\theta)(a - b)$. As H contains no nontrivial translations, we have $d = 0$. As $1 - R_\theta$ and $1 - R_\phi$ are invertible, we must have $a - b = 0$, and so $a = b$, so $f = R_{a,\phi}$. Thus the element $f = R_{a,\phi}$ has $f(a) = a$ as claimed.

Now suppose instead that f is a reflection, say $f = S_L$. We then note that the element $h = (R_{a,\theta}S_L)^2$ also lies in H. Part (a) of the lemma tells us that $h = T_c$, where $c = (1 - R_\theta)(a - S_L(a))$. It follows that $c = 0$, and $1 - R_\theta$ is invertible so $a - S_L(a) = 0$, so $S_L(a) = a$. Thus $f(a) = S_L(a) = a$ as required.

This proves the theorem when H contains a nontrivial rotation. Now suppose instead that H contains only reflections and the identity map. I claim that H contains at most one reflection. If not, let S_K and S_L be two different reflections in H, so $S_L S_K$ also lies in H. We see from parts (c) and (d) of the lemma that $S_L S_K$ is either a nontrivial translation or a nontrivial rotation, giving a contradiction. It follows that H is either the trivial group $\{1\}$ or a group of the form $\{1, S_L\}$ for some line L. In the first case we can take a to be any point at all, and in the second case a can be any point on L. □

Proof of Lemma 4.4. We first check the general type of the various isometries considered, using the method described in Remark 4.2.

(a) Clearly $\psi(R_{a,\theta}S_L)$ is a rotation times a reflection, which is another reflection. Every reflection in O_2 squares to the identity, so $\psi((R_{a,\theta}S_L)^2) = 1$, so $(R_{a,\theta}S_L)^2 = T_c$ for some c.

(b) We have

$$\psi(R_{a,\theta}R_{b,\phi}R_{a,\theta}^{-1}R_{b,\phi}^{-1}) = R_\theta R_\phi R_{-\theta} R_{-\phi} = R_{\theta+\phi-\theta-\phi} = 1,$$

so

$$R_{a,\theta}R_{b,\phi}R_{a,\theta}^{-1}R_{b,\phi}^{-1} = T_d$$

for some d.

(c) As L and K are parallel, they have the same angle with the x-axis, say α. We thus have

$$\psi(S_L S_K) = S_\alpha S_\alpha = 1,$$

so $S_L S_K = T_e$ for some e.

(d) Here $\psi(S_L S_K)$ is a product of two different reflections in O_2, so it is a rotation, say R_ϕ. This means that $S_L S_K = R_{a,\phi}$ for some a and ϕ.

We next find the details.

(a) To find c, we choose any convenient point x, and then c will be $c = (R_{a,\theta}S_L)^2(x) - x$. We will take $x = S_L(a)$. We then have $S_L(x) = a$ so $R_{a,\theta}S_L(x) = R_{a,\theta}(a) = a$ so

$$\begin{aligned}(R_{a,\theta}S_L)^2(x) &= R_{a,\theta}S_L(a)\\ &= R_\theta S_L(a) + (1 - R_\theta)a\\ c = (R_{a,\theta}S_L)^2(x) - x &\\ &= R_\theta S_L(a) + (1 - R_\theta)a - S_L(a)\\ &= (1 - R_\theta)a + (R_\theta - 1)S_L(a)\\ &= (1 - R_\theta)(a - S_L(a)).\end{aligned}$$

(b) Put $f = R_{a,\theta}R_{b,\phi}R_{a,\theta}^{-1}R_{b,\phi}^{-1}$. We have seen that $\psi(f) = 1$, so $f = T_d$ for some d. To find d, we choose any convenient point x, and then d will be $f(x) - x$. We will take $x = R_{b,\phi}R_{a,\theta}(b)$, so

$$\begin{aligned}f(x) &= R_{a,\theta}R_{b,\phi}R_{a,\theta}^{-1}R_{b,\phi}^{-1}R_{b,\phi}R_{a,\theta}(b)\\ &= R_{a,\theta}R_{b,\phi}(b)\\ &= R_{a,\theta}(b)\\ &= R_\theta b + (1 - R_\theta)a.\end{aligned}$$

(At the third step we used the fact that $R_{b,\phi}$ is a rotation around b, so it sends b to itself.)

We also have

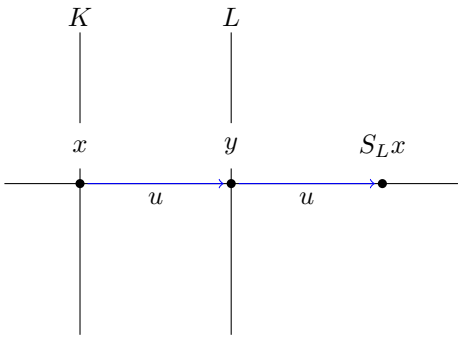
$$\begin{aligned}x &= R_{b,\phi}R_{a,\theta}(b)\\ &= R_{b,\phi}(R_\theta b + (1 - R_\theta)a)\\ &= R_\phi R_\theta b + R_\phi(1 - R_\theta)a + (1 - R_\phi)b.\end{aligned}$$

By subtracting these, we get

$$\begin{aligned}d &= f(x) - x\\ &= R_\theta b + (1 - R_\theta)a\\ &\quad -R_\phi R_\theta b - R_\phi(1 - R_\theta)a - (1 - R_\phi)b\\ &= (1 - R_\phi)R_\theta b + (1 - R_\phi)(1 - R_\theta)a - (1 - R_\phi)b\\ &= (1 - R_\phi)(1 - R_\theta)(a - b).\end{aligned}$$

(c) We know that $S_L S_K = T_e$ for some e. Choose any point x on the line K, so $S_K(x) = x$. We then have $e = S_L S_K(x) - x = S_L(x) - x$.

If we move away from x towards L in a direction perpendicular to K and L, we will eventually reach L. In other words, there is a vector u perpendicular to K and L such that the point $y := x + u$ lies in L. As L is parallel to K, it is easy to see that $L = K + u$. Moreover, $S_L(x)$ is the reflection of x across L, which is just $x + 2u$. It follows that $e = S_L(x) - x = 2u$ as claimed.



(d) Let K and L be lines that are not parallel. It is geometrically clear that they meet in a unique point, which we call a. Let α be the angle between the x-axis and K, measured anticlockwise from the axis. Let θ be the angle between K and L, measured anticlockwise from K, so that $\theta \in [0, \pi)$. Clearly L

is obtained by rotating K around a through an angle of θ, in other words $L = R_{a,\theta}K$. We also have $S_K = T_a S_{2\alpha} T_{-a}$ and $S_L = T_a S_{2\alpha+2\theta} T_{-a}$ and $S_{2\alpha+2\theta} S_{2\alpha} = R_{2\theta}$ so $S_L S_K = T_a R_{2\theta} T_{-a} = R_{a,2\theta}$.

□

Corollary 4.5. *Let H be a finite subgroup of* Isom_2. *Then either $H = T_a C_n T_a^{-1}$ for some a and n, or $H = T_a R_\theta D_n R_\theta^{-1} T_a^{-1}$ for some a, n and θ.*

Proof. Every element of H has finite order, and thus cannot be a nontrivial translation. It follows from the theorem that $H \leq T_a O_2 T_a^{-1}$ for some a, so the group $H' := T_a^{-1} H T_a$ is contained in O_2. Theorem 2.4 tells us that H' has the form C_n or $R_\theta D_n R_\theta^{-1}$ and clearly $H = T_a H' T_a^{-1}$. The claim follows. □

5. Wallpaper

In this section we study symmetry groups of "wallpaper patterns", which for our purposes will mean "reasonable" subsets of $\mathbb{R}^2$ which are translationally symmetric in two different directions. (I say "reasonable" to exclude sets like $\mathbb{Q}^2$; we will be more precise later.) The real importance of this study (and its three-dimensional analogue) is in the physical chemistry of crystals: the symmetry group of a crystal is a useful tool in studying the way it vibrates, refracts X-rays, and so on.

The simplest wallpaper group was discussed in Example 3.9. It turns out that there are precisely 17 types of wallpaper up to a suitable notion of equivalence. Here we will analyse a small selection of these types, and prove some of the key results in the general classification.

We start with some general concepts.

Definition 5.1. For any subgroup $H \leq \mathrm{Isom}_2$, the *point group* of H is the subgroup $\psi(H) = \{\psi(h) \mid h \in H\} \leq O_2$, where ψ is as in Section 3.1. We also write $\mathrm{Trans}(H) = \{a \in \mathbb{R}^2 \mid T_a \in H\}$ and call this the translation subgroup of H.

For any point $a \in \mathbb{R}^2$, we also define $\sigma_a(H) = \{A \in O_2 \mid T_a A T_a^{-1} \in H\}$, which is a subgroup of O_2. This is the part of H that encodes the rotational and reflectional symmetry about a.

Proposition 5.2. *For any $a \in A$ we have $\sigma_a(H) \subseteq \psi(H)$.*

Proof. If $A \in \sigma_a(H)$ then $T_a A T_a^{-1} \in H$, so $\psi(T_a)\psi(A)\psi(T_a)^{-1} \in \psi(H)$. We have $\psi(T_a) = I$ and $\psi(A) = A$, so $A \in \psi(H)$, as required. □

Definition 5.3. Let G be a group, and let $x_1, \dots, x_r$ be elements of G. We say that these elements *generate* G if every element in $g \in G$ can be expressed in terms of the elements x_i, say

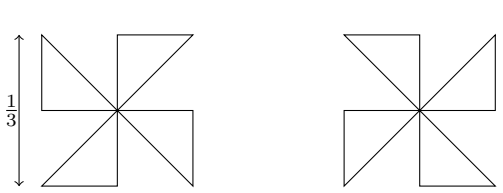
$$g = x_{i_1}^{n_1} x_{i_2}^{n_2} \cdots x_{i_r}^{n_r}$$

for some indices $i_1, \dots, i_r$ and integers $n_1, \dots, n_r$.

Equivalently, the x_i generate G iff the only subgroup of G containing all the x_i is G itself.

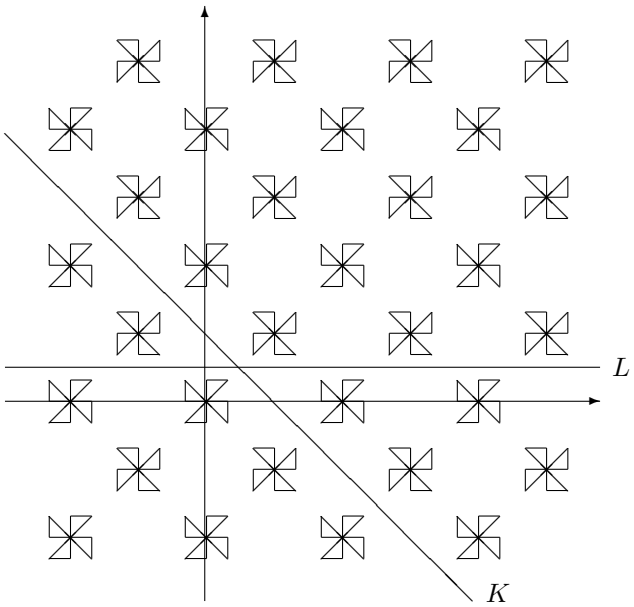
We will be interested in finding small sets of generators for some of the wallpaper groups.

5.1. **The group p4g.** Let M be the figure shown on the left below, and let M' be its mirror image, as shown on the right.



It is easy to see that $\mathrm{Symm}(M) = \mathrm{Dir}(M) = C_4$.

Now let X be the figure shown below, consisting of a copy of M centred at each point of the form (n, m) with $n, m \in \mathbb{Z}$, together with a copy of M' centred at each point of the form $(n + \frac{1}{2}, m + \frac{1}{2})$. We will study the group $\mathrm{Isom}(X) := \{f \in \mathrm{Isom}_2 \mid f(X) = X\}$, which is known in chemistry as p4g.



Let K and L be the lines marked in the diagram, so K has equation $x+y=\frac{1}{2}$ and L has equation $y=\frac{1}{4}$. We define isometries as follows:

$$\begin{array}{rll} T_1 & = T_{(1,0)} & (x,y) \mapsto (x+1,y) \\ T_2 & = T_{(0,1)} & (x,y) \mapsto (x,y+1) \\ G & = T_{(1/2,0)} S_L & (x,y) \mapsto (\tfrac{1}{2}+x, \tfrac{1}{2}-y) \\ R & = R_{\pi/2} & (x,y) \mapsto (-y,x) \\ S & = S_K & (x,y) \mapsto (\tfrac{1}{2}-y, \tfrac{1}{2}-x). \end{array}$$

I claim that X is invariant under all these isometries; this is clear by inspection. For example, if we reflect the pattern across L and then shift half a unit to the right, we get the original pattern back, which shows that $GX = X$.

Proposition 5.4. $\mathrm{Isom}(X)$ *is generated by* T_1, T_2, G *and* R.

Proof. Let H be the group generated by T_1, T_2, G and R. As these isometries preserve X, we have $H \leq \mathrm{Isom}(X)$. Now let f_0 be an arbitrary element of $\mathrm{Isom}(X)$. If $\det(f_0) = -1$ we define $f_1 = G^{-1} f_0$, otherwise we put $f_1 = f_0$. Either way we have $f_1 \in \mathrm{Isom}(X)$ and $\det(f_1) = 1$. It is geometrically obvious that f_1 must send the copy of M centred at $(0,0)$ to some other copy of M, and thus that $f_1(0,0) = (n,m)$ for some $n, m \in \mathbb{Z}$. Now put $f_2 = T_1^{-n} T_2^{-m} f_1$, so that $f_2 \in \mathrm{Isom}(X)$ and $\det(f_2) = 1$ and $f_2(0,0) = (0,0)$. This implies that $f_2 \in SO_2$, in other words f_2 is a rotation, and clearly the angle must be a multiple of $\pi/2$, so $f_2 = R^k$ for some k. Thus f_0 has the form $T_2^m T_1^n R^k$ or $G T_2^m T_1^n R^k$, which means that $f_0 \in H$. Thus $\mathrm{Isom}(X) \subseteq H$ as required. □

Corollary 5.5. $\mathrm{Isom}(X)$ *is generated by* R *and* S.

Proof. It will suffice to write the generators T_1, T_2 and G in terms of R and S. The relevant formulae are as follows:

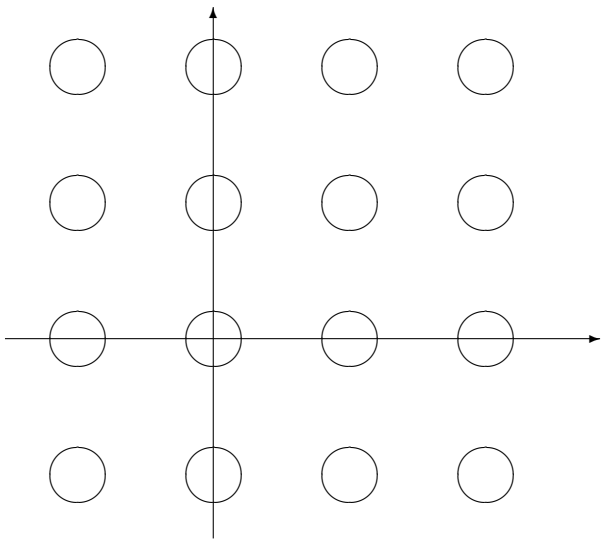
$$\begin{aligned} G &= SR^{-1} \\ T_1 &= G^2 = SR^{-1}SR^{-1} \\ T_2 &= RT_1R^{-1} = RSR^{-1}SR^{-2} \end{aligned}$$

These facts can be proved from the formulae given above in terms of x and y, or by geometric arguments. □

Remark 5.6. We have $\psi(T_1) = \psi(T_2) = I$ and $\psi(R) = R$ and $\psi(G) = S_0$. The group $\mathrm{Isom}(X)$ is generated by T_1, T_2, R and G, so $\psi(\mathrm{Isom}(X))$ is generated by R and S_0, so $\psi(\mathrm{Isom}(X)) = D_4$. On the other hand,

one checks that for each $a \in \mathbb{R}^2$, the group $\sigma_a(\mathrm{Isom}(X))$ is either C_1, C_2 or C_4. In particular, there is no point a for which $\sigma_a(\mathrm{Isom}(X)) = \psi(\mathrm{Isom}(X))$.

5.2. **The group p4m.** Let $C_{n,m}$ denote the circle of radius $1/3$ centred at (n, m), and let X denote the union of all the circle $C_{n,m}$ for $(n, m) \in \mathbb{Z}^2$.



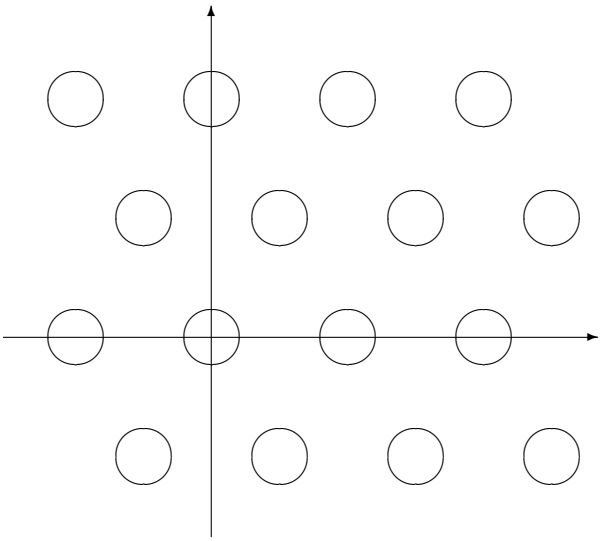
The symmetry type of this pattern is known as p4m.

Let T_1, T_2 and R be as before, and let S_0 denote reflection in the x-axis (as usual). These are easily seen to preserve X, and I claim that they generate $\mathrm{Isom}(X)$.

To see this, suppose that $f_0 \in \mathrm{Isom}(X)$. Then f_0 must send $C_{0,0}$ to one of the other circles in the pattern, say $f(C_{0,0}) = C_{n,m}$. Put $f_1 = T_1^{-n} T_2^{-m} f_0$, so that $f_1 \in \mathrm{Isom}(X)$ and $f_1(C_{0,0}) = C_{0,0}$. This means that f_1 is either a rotation around $(0, 0)$ or a reflection across a line through $(0, 0)$. If it is a rotation, the angle must clearly be a multiple of $\pi/2$, and thus $f_1 = R^k$ for some k. If it is a reflection, one sees by inspection that the slope of the line must be $k\pi/4$ for some k, and thus that $f_1 = S_{k\pi/2} = R^k S_0$. Thus $f_0 = T_1^n T_2^m R^k$ or $f_1 = T_1^n T_2^m R^k S_0$, as required.

In this case, the point group is generated by $\psi(T_1)$, $\psi(T_2)$, $\psi(R)$ and $\psi(S_0)$. We have $\psi(T_1) = \psi(T_2) = 1$ and $\psi(R) = R$ and $\psi(S_0) = S_0$, so the point group is generated by R and S_0 and thus is equal to D_4 again. In contrast to the p4g case, we have $\sigma_0(\mathrm{Isom}(X)) = D_4 = \psi(\mathrm{Isom}(X))$.

5.3. **The group p6m.** Put $u = (1, 0)$ and $v = R_{\pi/6}(u) = (1/2, \sqrt{3}/2)$, so that 0, u and v are the vertices of an equilateral triangle of side 1. Let $C_{n,m}$ be a circle of radius $1/3$ centred at $nu + mv$, and let X be the union of the circles $C_{n,m}$



This can be analysed in much the same way as the previous example. We find that $\mathrm{Isom}(X)$ is generated by T_u, T_v, $R_{\pi/3}$ and S_0. The point group is D_6, which is the same as $\sigma_0 \mathrm{Isom}(X)$.

5.4. **Steps towards the classification.** We will adopt the following definition.

Definition 5.7. A *wallpaper group* or *two-dimensional crystallographic group* is a subgroup $H \leq \mathrm{Isom}_2$ such that

(a) $\psi(H)$ is finite.
(b) There exist linearly independent vectors $u, v \in \mathrm{Trans}(H)$ such that every vector in $\mathrm{Trans}(H)$ can be written as $nu + mv$ for some $n, m \in \mathbb{Z}$.

It is usual to use a somewhat different definition, which can be shown to be equivalent to that given above.

Let H be a wallpaper group. We say that H is *oriented* if $\psi(H) \leq SO_2$; if so, we know from Theorem 2.4 that $\psi(H) = C_n$ for some n. We call n the *rotational order* of H.

Now suppose that H is not oriented, so $\psi(H) = R_\theta D_n R_\theta^{-1}$ for some n and θ. We again call n the rotational order of H.

Lemma 5.8. *If $A \in \psi(H)$ and $b \in \mathrm{Trans}(H) \subset \mathbb{R}^2$ then $Ab \in \mathrm{Trans}(H)$.*

Proof. As $b \in \mathrm{Trans}(H)$ we have $T_b \in H$. As $A \in \psi(H)$, there is an element $f \in H$ of the form $f(x) = Ax + c$ for some c. It follows that $fT_bf^{-1} \in H$, and we see from Proposition 3.7 that $fT_bf^{-1} = T_{Ab}$, so $Ab \in \mathrm{Trans}(H)$. □

To explain what the next lemma is about, consider the group $V \leq \mathbb{R}^2$ consisting of vectors of the form $n(-1, 0) + m(\sqrt{2}, 0)$ with $n, m \in \mathbb{Z}$. We can choose a rational number n/m which is a very good (but not perfect) rational approximation to $\sqrt{2}$, and we find that $n(-1, 0) + m(\sqrt{2}, 0)$ is very small (but nonzero). By making this precise, we find that for any $\epsilon > 0$ there exists $v \in V \setminus \{0\}$ such that $\|v\| < \epsilon$. Thus, there is no shortest vector in $V \setminus \{0\}$. This phenomenon can only happen because $(-1, 0)$ and $(\sqrt{2}, 0)$ are linearly dependent vectors; in particular, it does not occur in $\mathrm{Trans}(H)$. The point of the next lemma is to prove this.

Lemma 5.9. *If H is a wallpaper group then there exists $w \in \mathrm{Trans}(H) \setminus \{0\}$ such that $\|b\| \geq \|w\|$ for all $b \in \mathrm{Trans}(H) \setminus \{0\}$.*

Proof. Let u and v be as in Definition 5.7. We claim that there is a positive constant $K > 0$ such that

$$\|nu + mv\| \geq \sqrt{n^2 + m^2}/K.$$

To see this, define $f\colon [0, 2\pi] \to \mathbb{R}$ by $f(\theta) = \|\cos(\theta)u + \sin(\theta)v\|$. As u and v are linearly independent we have $\cos(\theta)u + \sin(\theta)v \neq 0$ and thus $f(\theta) > 0$ for all θ. It follows that $1/f$ is a positive continuous function

on the closed interval $[0, 2\pi]$, so $1/f$ is bounded by some number $K > 0$, so $f(\theta) \geq 1/K$ for all θ. Now, for any n and m we can write $(n, m) = r(\cos(\theta), \sin(\theta))$ for some θ, where $r = \sqrt{n^2 + m^2}$. This means that

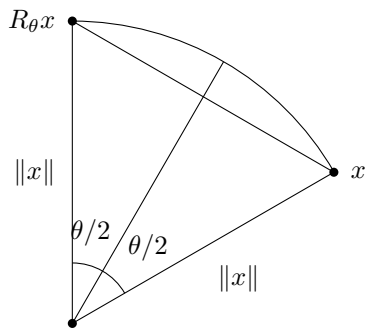
$$\begin{aligned} \|nu + mv\| &= \|r(\cos(\theta)u + \sin(\theta)v)\| \\ &= rf(\theta) \geq r/K = \sqrt{n^2 + m^2}/K, \end{aligned}$$

as claimed.

Now consider a disc D of radius R centred at the origin, and put $S = (\mathrm{Trans}(H) \setminus \{0\}) \cap D$, the set of nonzero vectors in $\mathrm{Trans}(H)$ of length at most R. We choose R large enough that D contains at least one of the nonzero points in $\mathrm{Trans}(H)$, so $S \neq \emptyset$. If $nu + mv \in S$ then $R \geq \|nu + mv\| \geq \sqrt{n^2 + m^2}/K$, so $|n|, |m| \leq RK$. This means that there are only finitely many possibilities for n and m, so there are only finitely many points in S. Among this finite list of points, we choose one that is as close as possible to zero, and call it w. This clearly has the required property. □

Theorem 5.10. *The rotational order of H is 1, 2, 3, 4 or 6.*

Proof. Let n be the rotational order, so the element $R := R_{2\pi/n}$ lies in $\psi(H)$. Let $w \in \mathrm{Trans}(H)$ be as in Lemma 5.9. Lemma 5.8 tells us that $R(w) \in \mathrm{Trans}(H)$ and $\mathrm{Trans}(H)$ is a subgroup of $\mathbb{R}^2$ so $R(w) - w \in \mathrm{Trans}(H)$, so $\|R(w) - w\| \geq \|w\|$ by the definition of w. However, for any x and θ we have $\|R_\theta(x) - x\| = 2\sin(\theta/2)\|x\|$, as we see from the diagram below.



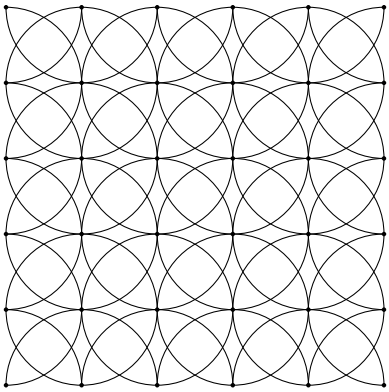
It follows that $\|R(w) - w\| = 2\sin(\pi/n)\|w\|$, so we must have $2\sin(\pi/n) \geq 1$, so $\sin(\pi/n) \leq 1/2 = \sin(\pi/6)$, so $n \leq 6$.

All that is left is to show that the case $n = 5$ leads to a contradiction, which we do by a variation of the preceeding argument. Clearly $w + R^{-2}w \in \mathrm{Trans}(H)$, but if $n = 5$ then $-R^{-2}w = R_\pi R_{-4\pi/5} = R_{\pi/5}w$ so $\|w + R^{-2}w\| = \|w - R_{\pi/5}w\| = 2\sin(\pi/10)\|w\| < \|w\|$, which contradicts our choice of w, as required. □

Proposition 5.11. *Suppose that H has rotational order n, where $n \in \{3, 4, 6\}$. Let w be as in Lemma 5.9, and put $x = R_{2\pi/n}(w)$. Then $\mathrm{Trans}(H) = \{pw + qx \mid p, q \in \mathbb{Z}\}$.*

Proof. Put $L = \{pw + qx \mid p, q \in \mathbb{Z}\} \leq \mathrm{Trans}(H)$ and $r = \|w\|$. I claim that for each $a \in \mathbb{R}^2$, there exists $b \in L$ such that $d(a, b) < r$. Assuming this, when $a \in \mathrm{Trans}(H)$ we have $a - b \in \mathrm{Trans}(H)$ and $\|a - b\| < r$ so $a - b = 0$ by our choice of w, so $a = b$; this proves that $\mathrm{Trans}(H) = L$ as required.

To prove the claim, we first consider the case $n = 4$, where w and x are orthogonal. After a suitable change of coordinates we have $w = (r, 0)$ and $x = (0, r)$, and the claim is that every point in $\mathbb{R}^2$ lies in the open ball of radius r centred at (pr, qr) for some $p, q \in \mathbb{Z}$. This should be geometrically clear from the following diagram.

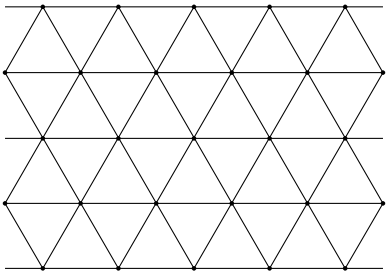


For an algebraic proof, note that $\{w, x\}$ is a basis for $\mathbb{R}^2$, so any vector $a \in \mathbb{R}^2$ can certainly be written in the form $pw + qx$ for some $p, q \in \mathbb{R}$. We can choose $p', q' \in \mathbb{Z}$ with $|p - p'| \leq \frac{1}{2}$ and $|q - q'| \leq \frac{1}{2}$, and then put $b = p'w + q'x \in L$. We then have $a - b = (p - p')w + (q - q')x$ and w and x are orthogonal so

$$\|a - b\|^2 = (p - p')^2 r^2 + (q - q')^2 r^2 \leq (\tfrac{1}{4} + \tfrac{1}{4})r^2 < r^2,$$

so $\|a - b\| < r$ as required.

We next turn to the case $n = 6$. It should be clear from the way the previous case worked that the value of r is irrelevant, so we assume that $r = 1$. We may also change coordinates and assume that $w = (1, 0)$, so $x = R_{2\pi/6}w = (1/2, \sqrt{3}/2)$. The lattice L consists of the dots in the following diagram:



Each of the triangles is equilateral with side 1, and every point in such a triangle lies at distance < 1 from at least one of the vertices. (In fact, if T is an equilateral triangle of side 1 with vertices A, B and C and $X \in T$ then the distances $d(A, X)$, $d(B, X)$ and $d(C, X)$ are *all* less than one unless X is itself a vertex; in the exceptional case, of course X lies at distance 0 from one of the vertices.) This settles the case $n = 6$.

Finally, we treat the case $n = 3$. With assumptions as in the case $n = 6$, we have $w = (1, 0)$ and $x = R_{2\pi/3}(w) = (-1/2, \sqrt{3}/2)$. Put $y = R_{2\pi/6}(w) = (1/2, \sqrt{3}/2)$ and notice that $y = x + w$ and $x = y - w$. This shows that every integer combination of w and x is an integer combination of w and y, and *vice versa*. This means that the lattice for the $n = 3$ case is exactly the same as for the $n = 6$ case, so again every point in $\mathbb{R}^2$ is at distance < 1 from a lattice point. □

We now see that $\psi(H)$ is conjugate to C_n or D_n where $n \in \{1, 2, 3, 4, 6\}$, which gives twelve possibilities for $\psi(H)$. In the cases $n \geq 3$ we have a strong information about $\mathrm{Trans}(H)$. Even if we know $\psi(H)$ and $\mathrm{Trans}(H)$ there may be more than one possibility for H, as exemplified by the difference between p4g and p4m. Nonetheless, we are well on the way to the complete classification of wallpaper groups.

6. Polyhedra

We now turn to the study of symmetries in three dimensions. In this context we will not consider translations, so we are really just looking at subgroups of O_3. It will turn out that this is strongly related to the theory of regular polyhedra, otherwise known as Platonic solids.

6.1. **Actions of groups on sets.** In our study of subgroups of O_3 (and in later sections of the course) it will be helpful to think about actions of groups on sets.

Definition 6.1. Let G be a group and X a set. An *action* of G on X is a rule which assigns to each element $g \in G$ and each element $x \in X$ an element $g * x \in X$, such that

A1 $1 * x =$ for all $x \in X$
A2 $g * (h * x) = (gh) * x$ for all $g, h \in G$ and $x \in X$.

We will often write gx for $g * x$.

Example 6.2. Put $X = S^2 = \{x \in \mathbb{R}^3 \mid \|x\| = 1\}$. If $x \in S^2$ and $A \in O_3$ then $Ax \in S^2$. Clearly $Ix = x$ and $(AB)x = A(Bx)$, so this gives an action of O_3 on S^2.

Example 6.3. Consider the group $G = D_4 = \{1, R, R^2, R^3, S, RS, R^2S, R^3S\}$, where $R = R_{\pi/2}$ and $S = S_0$. Let L_0 be the line with equation $x = y$, and let L_1 be the line with equation $x = -y$. One checks that $S(L_0) = L_1$ and $S(L_1) = L_0$, and similarly $R(L_0) = L_1$ and $R(L_1) = L_0$. It follows that for each $g \in D_4$ we either have $g(L_0) = L_0$ or $g(L_0) = L_1$, and similarly we either have $g(L_1) = L_1$ or $g(L_1) = L_0$. Thus, if we put $X = \{L_0, L_1\}$ then D_4 acts on X.

Example 6.4. Let G be any group. For any $g, x \in G$ we define $g * x = gxg^{-1}$. This satisfies $1 * x = x$ and

$$g * (h * x) = g * (hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = (gh) * x.$$

Thus, we have an action of G on itself, called the *conjugation action*. In this case it would of course be a mistake to write gx instead of $g * x$.

We next introduce a different way of thinking about group actions.

Definition 6.5. A *permutation* of a set X is a bijective function $\sigma\colon X \to X$. We write $S(X)$ for the group of all permutations of X, and we write $S_n = S(\{1, \dots, n\})$.

Suppose we have an action of G on X. For any $g \in G$, we can define a function $\phi(g)\colon X \to X$ by $\phi(g)(x) = g * x$. This satisfies $\phi(1)(x) = 1 * x = x$, so $\phi(1)$ is the identity map. Moreover, we have

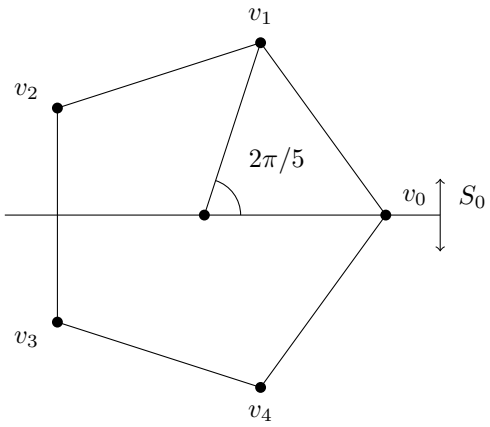
$$(\phi(g) \circ \phi(h))(x) = \phi(g)(\phi(h)(x)) = g * (h * x) = (gh) * x = \phi(gh)(x),$$

so $\phi(gh) = \phi(g) \circ \phi(h)$. In particular, we have $\phi(g)\phi(g^{-1}) = \phi(1) = 1$, and similarly $\phi(g^{-1})\phi(g) = 1$. Thus $\phi(g)$ is a bijection, with inverse $\phi(g^{-1})$. We have thus defined a homomorphism $\phi\colon G \to S(X)$. Conversely, if we start with a homomorphism $\phi\colon G \to S(X)$ we can define an action by $g * x = \phi(g)(x)$. Thus, actions of G on X are essentially the same as homomorphisms from G to $S(X)$.

Example 6.6. Let $V = \{v_0, v_1, v_2, v_3, v_4\}$ be the set of vertices of the standard pentagon, so the group D_5 acts on V, giving a homomorphism $\phi\colon D_5 \to S(V)$. If we write $R = R_{2\pi/5}$ and $S = S_0$ as usual then

$$\begin{aligned}
\phi(R)(v_0) &= v_1 \\
\phi(R)(v_1) &= v_2 \\
\phi(R)(v_2) &= v_3 \\
\phi(R)(v_3) &= v_4 \\
\phi(R)(v_4) &= v_0.
\end{aligned}$$

We can write this in cycle notation as $\phi(R) = (v_0\ v_1\ v_2\ v_3\ v_4)$. If we identify V with $\{0, 1, 2, 3, 4\}$ in the obvious way then $\phi(R)$ becomes the permutation (0 1 2 3 4). Similarly, we have $\phi(S) = (1\ 4)(2\ 3)$.



6.2. **Rotations and axes.** We have already seen a very simple and concrete description of the elements of SO_2; they are just the rotations R_θ for $0 \leq \theta \leq 2\pi$. Our next task is to see how far this generalises to SO_3, or to SO_n for $n > 3$.

Proposition 6.7. *If $A \in SO_n$ and n is odd then 1 is an eigenvalue of A.*

Proof. We have $A^T = A^{-1}$, so

$$A^T(A - I) = I - A^T = -(A - I)^T.$$

For any $n \times n$ matrix B we have $\det(B^T) = \det(B)$ and $\det(-B) = (-1)^n \det(B) = -\det(B)$ (as n is odd). We can thus take determinants in the displayed equation to get

$$\det(A)\det(A - I) = -\det(A - I).$$

As $A \in SO_n$ we have $\det(A) = 1$ so $\det(A - I) = -\det(A - I)$, so $\det(A - I) = 0$ as required. □

Corollary 6.8. *If $A \in SO_3$ then there is an orthonormal basis $\{u, v, w\}$ of $\mathbb{R}^3$ and an angle θ such that*

$$\begin{aligned} Au &= u \\ Av &= \cos(\theta)v + \sin(\theta)w \\ Aw &= -\sin(\theta)v + \cos(\theta)w. \end{aligned}$$

Thus, A is conjugate in O_3 to a matrix of the form

$$U_\theta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Proof. As 1 is an eigenvalue, there is a vector $u' \neq 0$ such that $Au' = u'$. Put $u = u'/\|u'\|$, so $\|u\| = 1$ and $Au = u$. Let v be any unit vector perpendicular to u, and let w be either of the two unit vectors that are perpendicular to the plane spanned by u and v. As $Au = u$ and A preserves inner products, we have $\langle Av, u\rangle = \langle Av, Au\rangle = \langle v, u\rangle = 0$, so Av is perpendicular to u. It is clear that v and w form a basis for the plane perpendicular to u, so $Av = cv + sw$ for some $c, s \in \mathbb{R}$. Moreover, we have

$$1 = \|v\|^2 = \|Av\|^2 = \langle cv + sw, cv + sw\rangle = c^2 + s^2,$$

so we have $(c, s) = (\cos(\theta), \sin(\theta))$ for some θ. Similarly, we have $Aw = c'v + s'w$ for some c', s' with $(c')^2 + (s')^2 = 1$. As $\langle v, w\rangle = 0$ we have $\langle Av, Aw\rangle = 0$ and thus $cc' + ss' = 0$. Thus (c', s') is a unit vector in $\mathbb{R}^2$ which is orthogonal to (c, s); one sees easily that the only possibilities are $(c', s') = (-s, c)$ and $(c', s') = (s, -c)$. For the moment we simply assume that $(c', s') = (-s, c)$; we will explain later why the other case is impossible. Define $\beta\colon \mathbb{R}^3 \to \mathbb{R}^3$ by $\beta(x, y, z) = xu + yv + zw$. As u, v and w are orthonormal we see that

$$\|\beta(x, y, z)\|^2 = \langle xu + yv + zw, xu + yv + zw\rangle = x^2 + y^2 + z^2 = \|(x, y, z)\|^2.$$

Thus β is a norm-preserving linear map, so the corresponding matrix B is orthogonal. We have

$$\begin{aligned} AB(x,y,z) &= A(xu + yv + zw) \\ &= xAu + yAv + zAw \\ &= xu + y(cv + sw) + z(-sv + cw) \\ &= xu + (cy - sz)v + (sy + cz)w \\ &= BU_\theta(x,y,z), \end{aligned}$$

so $B^{-1}AB = U_\theta$. Thus A is conjugate to U_θ in O_3, as claimed.

Now suppose instead that $(c', s') = (s, -c)$. Then we would have $B^{-1}AB = U'_\theta$, where U'_θ is obtained from U_θ by multiplying the last column by -1. However, we have $A \in SO_3$ by assumption, so $\det(B^{-1}AB) = \det(B)^{-1}\det(A)\det(B) = 1$. We see by direct calculation that $\det(U'_\theta) = -1$, and this gives a contradiction. Thus we must have $(c', s') = (-s, c)$ after all. □

Proposition 6.9. *Suppose that $A \in SO_3$ and that there are two linearly independent vectors u and v such that $Au = u$ and $Av = v$. Then $A = I$.*

Proof. If A is not the identity, then it must be a nontrivial rotation, around an axis L say. This means that A fixes all the points on L, and moves all other points. As $Au = u$ and $Av = v$, we see that u and v must both lie on the line L. This is impossible, because they are linearly independent. □

Proposition 6.10. *If $G \leq O_3$ and $-1 \in G$ and $H = G \cap SO_3$ then $G = H \times \{\pm 1\}$.*

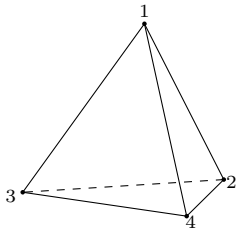
Proof. Define $\mu\colon H \times \{\pm 1\} \to G$ by $\mu(A, t) = tA$. As multiplication by any number commutes with multiplication by any matrix, we have

$$\mu(A,t)\mu(A',t') = tAt'A' = tt'AA' = \mu(AA', tt'),$$

so μ is a homomorphism. Suppose that $\mu(A,t) = I$; then either $A = I$ and $t = 1$ or $A = -I$ and $t = -1$, but the second case is impossible because $-I \notin SO_3$. This shows that $\ker(\mu)$ is the trivial group, so μ is injective. Next consider an element $B \in G$. If $\det(B) = 1$ then $B \in H$ so $B = \mu(B, 1)$ so B is in the image of μ. If $\det(B) = -1$ then $-B \in G$ (because B and -1 both lie in G) and $\det(-B) = 1$ so $-B \in H$. We also have $B = \mu(-B, -1)$, so we again see that B is in the image of μ. This shows that μ is surjective as well as injective, so it is an isomorphism of groups. □

Corollary 6.11. *In particular, we have $O_3 = SO_3 \times \{\pm 1\}$ as groups.* □

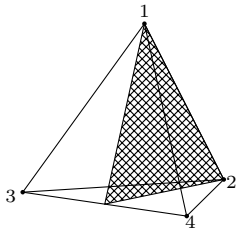
6.3. **Symmetries of the tetrahedron.** Let Tet be a regular tetrahedron centred at the origin, whose edges have length 1, and let $v_1, \dots, v_4$ be the vertices of Tet.



The action of Symm(Tet) on the vertices gives rise to a homomorphism $\phi\colon$ Symm(Tet) $\to S_4$. For example, let g be a 1/3-twist about the z-axis, anticlockwise as seen from above. Then g fixes v_1 and sends v_2 to v_3, v_3 to v_4 and v_4 back to v_2. Thus $\phi(g)$ is the 3-cycle (2 3 4).

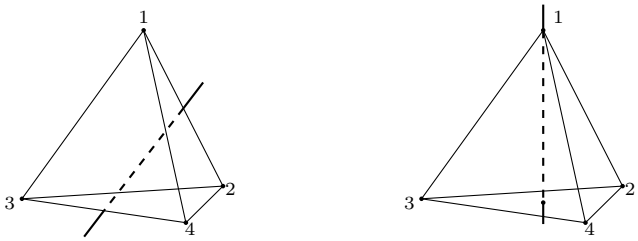
Theorem 6.12. *The homomorphism $\phi\colon$ Symm(Tet) $\to S_4$ is an isomorphism, and it also gives an isomorphism* Dir(Tet) $\to A_4$.

Proof. Given any pair of vertices v_i, v_j, let v_k and v_l be the two remaining vertices, and let P be the plane through v_k, v_l and $(v_i + v_j)/2$. Let A be the reflection across P (if n is a unit normal to P then A is given by $Ax = x - 2\langle n, x\rangle n$.) We find that $Av_i = v_j$ and $Av_j = v_i$, and that v_k and v_l are fixed by A. Thus $\phi(A)$ is the transposition $(i\ j)$. The diagram below illustrates the case $i = 3$, $j = 4$.

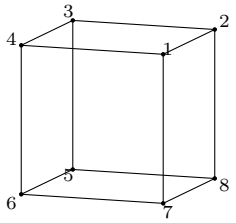


The image of ϕ is a subgroup of S_4 containing all the transpositions, and any permutation can be written as a product of transpositions, so the image is all of S_4, so ϕ is surjective. If $A \in \ker(\phi)$ then $Av_i = v_i$ for all i. It is easy to see that $\{v_1, v_2, v_3\}$ is a basis of $\mathbb{R}^3$ so we can conclude that $A = I$. This proves that ϕ is injective as well as surjective, so it is an isomorphism. We have seen that ϕ^{-1} sends each transposition to a reflection, so it sends any product of n transpositions to a product of n reflections, and we see that $\det(\phi^{-1}(\sigma)) = \operatorname{sgn}(\sigma)$ for all $\sigma \in S_4$, so ϕ^{-1} carries A_4 to Dir(Tet). By putting $\sigma = \phi(g)$ we deduce that $\operatorname{sgn}(\phi(g)) = \det(g)$, so ϕ carries Dir(Tet) to A_4. Thus ϕ gives an isomorphism $\mathrm{Dir(Tet)} \simeq A_4$ as claimed. □

Remark 6.13. If g is a half turn around the axis shown on the left, then $\phi(g)$ is the permutation (1 2)(3 4). If h is a one-third turn around the axis shown on the right, turning anticlockwise as seen from above, then $\phi(h) = (2\ 3\ 4)$. Note that this rotation looks clockwise when seen from below.



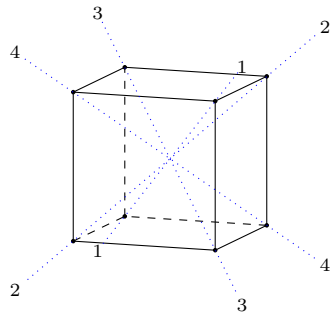
6.4. **Symmetries of the cube.** We now study the symmetries of a cube. We take our standard cube to have vertices $(\pm 1, \pm 1, \pm 1)$, so the centre is at $(0, 0, 0)$ and the edges have length 2.



We have marked the vertices so that the vertex labelled i is opposite the one labelled $i + 4$, which will be convenient later.

Note that (x, y, z) lies in the cube if and only if $(-x, -y, -z)$ does, so $-1 \in$ Symm(Cube) (the corresponding thing is *not* true for the tetrahedron). We therefore see from Proposition 6.10 that $\mathrm{Symm(Cube)} = \{\pm 1\} \times \mathrm{Dir(Cube)}$, so we will focus attention on Dir(Cube).

The action of Dir(Cube) on the eight vertices gives rise to an injective homomorphism $\mathrm{Dir(Cube)} \to S_8$, but it turns out that this is far from being surjective. In fact, $|\mathrm{Dir(Cube)}| = 4! = 24$ whereas $|S_8| = 8! = 40320$, so the image of our homomorphism is a rather small subgroup of S_8. We therefore use a different approach to study Dir(Cube). Let L_1, L_2, L_3 and L_4 be the four long diagonals of the cube, as shown below.



Note that L_i passes through v_i and v_{i+4}.

If $g \in \mathrm{Dir(Cube)}$ then g must send each long diagonal to another long diagonal, so Dir(Cube) acts on $\{L_1, L_2, L_3, L_4\}$. We therefore have a homomorphism $\phi\colon \mathrm{Dir(Cube)} \to S_4$ such that $g(L_i) = L_{\phi(g)(i)}$.

Lemma 6.14. *The homomorphism ϕ is injective.*

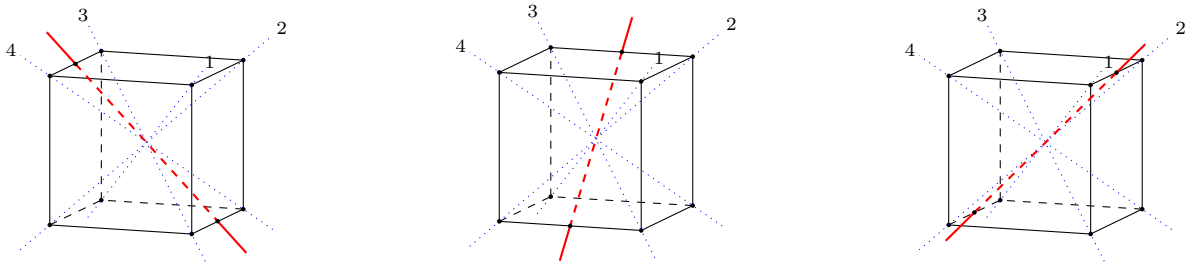
Proof. Suppose that $g \in \mathrm{Dir(Cube)}$ and that $\phi(g) = 1$; we must show that $g = 1$. Because $\phi(g) = 1$ we have $g(L_i) = L_i$ for all i. In particular, we have $v_1 \in L_1$ so $g(v_1) \in g(L_1) = L_1$, so either $g(v_1) = v_1$ or $g(v_1) = v_5 = -v_1$. Thus $g(v_1) = \epsilon_1 v_1$ for some $\epsilon_1 \in \{1, -1\}$, and similarly we have $g(v_i) = \epsilon_i v_i$ for some $\epsilon_i \in \{1, -1\}$ for $i = 2, 3, 4$.

Now suppose that $\epsilon_1 = \epsilon_2 = \epsilon_3 = -1$, so $g(v_1) = -v_1$, $g(v_2) = -v_2$ and $g(v_3) = -v_3$. As v_1, v_2 and v_3 are linearly independent (they do not all lie in any plane through the origin), they form a basis of $\mathbb{R}^3$. Given this, it is clear that $g = -1$, so $\det(g) = -1$, contradicting the assumption that $g \in \mathrm{Dir(Cube)} \leq SO_3$. So we cannot have $\epsilon_1 = \epsilon_2 = \epsilon_3 = -1$ after all.

More generally, any three of $\{v_1, v_2, v_3, v_4\}$ form a basis, so no three of the ϵ's can be -1. Thus at most two of the ϵ's are -1, so at least two of them are $+1$, say $\epsilon_i = \epsilon_j = 1$ with $i \neq j$. This means that $g(v_i) = v_i$ and $g(v_j) = v_j$, so g has two linearly independent fixed points. If g were a nontrivial rotation then all the fixed points would lie on the axis and thus any two would be linearly dependent. Thus g must be the identity. □

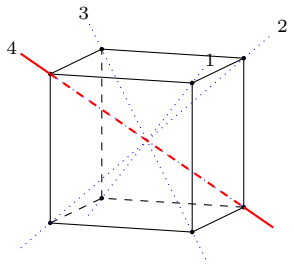
Theorem 6.15. *The homomorphism $\phi\colon \mathrm{Dir(Cube)} \to S_4$ is an isomorphism.*

Proof. Let g be a half turn around the axis shown on the left below. It is clear that g exchanges L_3 and L_4. The line L_1 is perpendicular to the axis of g, so when we perform the half turn we send L_1 to itself, just reversing the direction. Thus $g(L_1) = L_1$. Similarly, we have $g(L_2) = L_2$ and so $\phi(g) = (3\ 4)$.

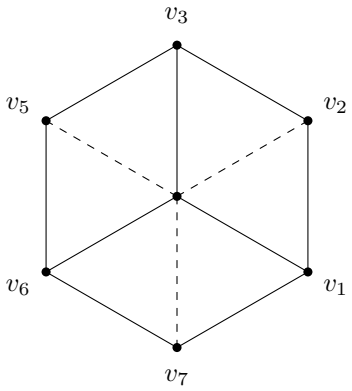


Similarly, if we do a half turn about the other two axes we get the transpositions (2 3) and (1 2). The transpositions (1 2), (2 3) and (3 4) lie in the image of ϕ and generate S_4, so ϕ is surjective. We have already seen that it is injective, so it must be an isomorphism. □

Remark 6.16. Let h be a one-third turn about L_4, rotating clockwise as seen from above.



If we look down L_4 at the cube we see the following picture:

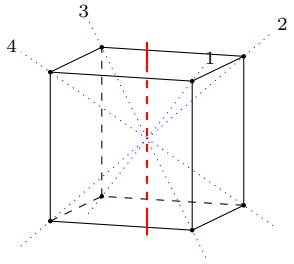


Thus h gives the following permutation of vertices:

$$v_1 \mapsto v_6 \mapsto v_3 \mapsto v_1$$
$$v_5 \mapsto v_2 \mapsto v_7 \mapsto v_5$$

As L_1 joins v_1 to v_5, L_2 joins v_6 to v_2 and L_3 joins v_3 to v_7 we see that the permutation of L's is $L_1 \mapsto L_2 \mapsto L_3 \mapsto L_1$, so $\phi(h) = (1\ 2\ 3)$.

Now let k be a quarter turn around the z-axis, anticlockwise as seen from above.

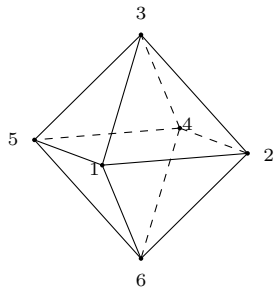


We then have $\phi(k) = (1\ 2\ 3\ 4)$ and $\phi(k^2) = (1\ 3)(2\ 4)$. We have thus found rotations giving representatives of all the cycle types in S_4.

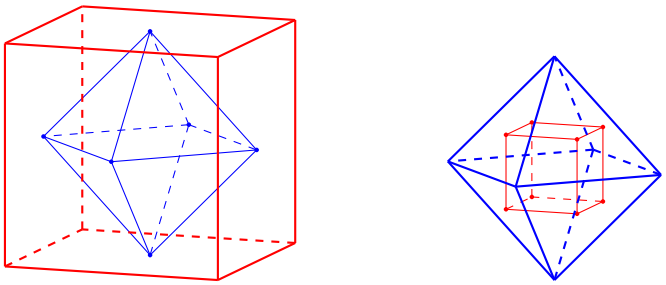
7. Duality and the Octahedron

We next study the symmetries of the octahedron. We take our standard octahedron to have vertices as follows:

$$w_1 = (1,0,0) \qquad w_2 = (0,1,0) \qquad w_3 = (0,0,1)$$
$$w_4 = (-1,0,0) \qquad w_5 = (0,-1,0) \qquad w_6 = (0,0,-1).$$



It turns out that there is a close relationship (called "duality") between the cube and the octahedron. As illustrated in the picture on the left, the vertices of the octahedron are the centres of the faces of the cube.



To see this algebraically, note that the vertices of the top face of the cube are $(1,1,1)$, $(-1,1,1)$, $(1,-1,1)$ and $(-1,-1,1)$. Thus, the centre of the top face is

$$\frac{1}{4}((1,1,1)+(-1,1,1)+(1,-1,1)+(-1,-1,1))=(0,0,1).$$

This is just the top vertex of the octahedron. The calculation for the other faces follows the same pattern.

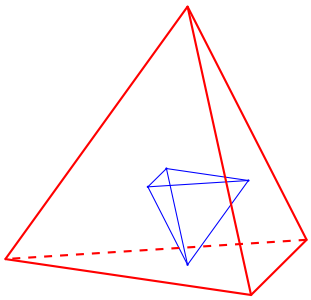
On the other hand, the centres of the faces of the octahedron are the vertices of a cube one third as big as the one we started with, as illustrated in the picture on the right.

Proposition 7.1. *The group* Symm(Oct) *is the same as* Symm(Cube) *(and thus is isomorphic to* $S_4\times\{\pm1\}$*).*

Proof. Suppose that $g\in$ Symm(Cube). Let w be a vertex of the octahedron. Then w is the centre of some face F of the cube. As g is a symmetry of the cube, gF is another face, and gw is the centre of gF, so gw is a vertex of the octahedron. Thus g sends vertices of the octahedron to vertices, and it follows that it sends the octahedron to itself. Thus Symm(Cube) $\subseteq$ Symm(Oct).

Now suppose that $h\in$ Symm(Oct). Let v be a vertex of the large cube, so $v/3$ is a vertex of the small cube, so $v/3$ is the centre of some face F' of the octahedron. As h is a symmetry of the octahedron, hF' is another face, and $h(v/3)$ is the centre of hF', so $h(v)/3=h(v/3)$ is a vertex of the small cube, so $h(v)$ is a vertex of the large cube. Thus h sends vertices of the cube to vertices, and it follows that it sends the cube to itself. Thus Symm(Oct) $\subseteq$ Symm(Cube). □

Remark 7.2. You might hope that a similar picture would give interesting information about the tetrahedron. However, the centres of the faces of a tetrahedron are just the vertices of a smaller tetrahedron, as illustrated below, so we just conclude that the two different tetrahedra have the same symmetry group.

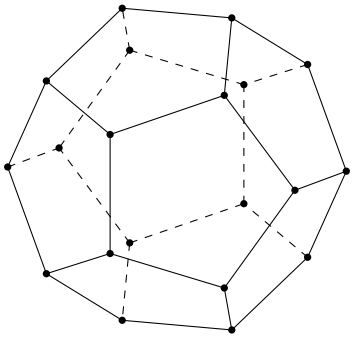


For an algebraic approach to this, note that the centre of the tetrahedron is $(v_1 + v_2 + v_3 + v_4)/4$, but by assumption the centre is at the origin, so we must have $v_1 + v_2 + v_3 + v_4 = 0$. The vertices of the face opposite v_1 are v_2, v_3 and v_4 so the centre of the face is $(v_2 + v_3 + v_4)/3 = -v_1/3$. More generally, the centre of the face opposite v_k is $-v_k/3$, and the points $-v_1/3$, $-v_2/3$, $-v_3/3$ and $-v_4/3$ clearly form a tetrahedron one third as big as the one we started with.

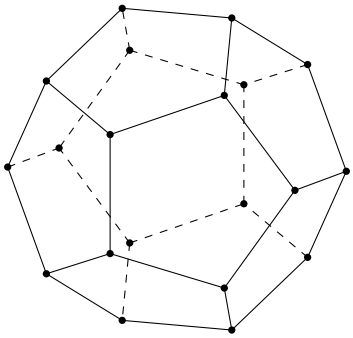
8. The construction of the dodecahedron

Proposition 8.1. *There is a solid (called the dodecahedron) with* 12 *faces, each of which is a regular pentagon with edges of length* 1.

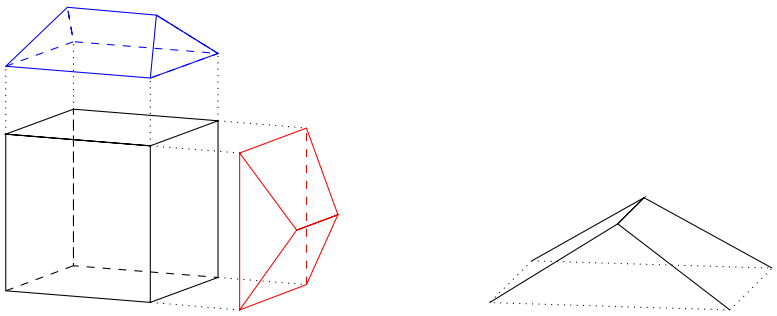
The rest of this section will constitute the proof; a picture of the dodecahedron is shown below.



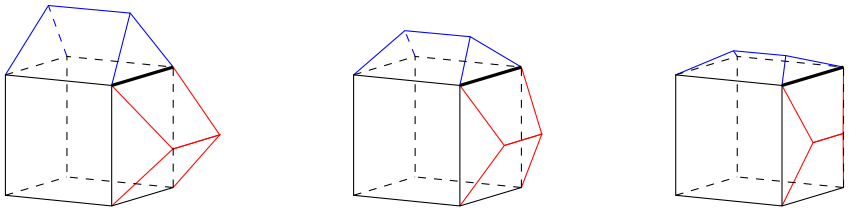
We will construct the dodecahedron by attaching "tents" to a cube as shown below. We have only shown two tents here but eventually we will use six tents, one for each face.



The edges of the cube will have length d; later on we will work out exactly what d has to be. The tents will be as shown below, with dotted edges of length d and solid edges of length 1.

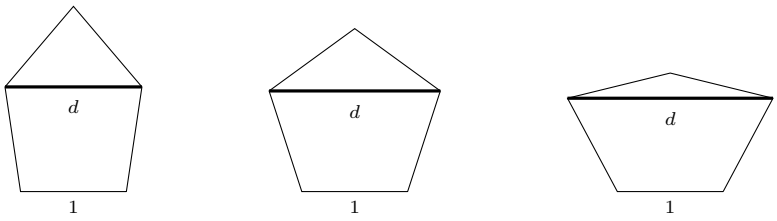


The next diagram shows the result of attaching tents to cubes of three different sizes.



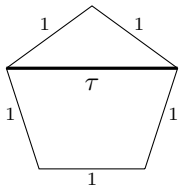
Note that we have a bent pentagon with the thick line cutting across it. If d is small as shown on the left, then the pentagon is bent outwards along the thick line. If d is too large as shown on the right, then the pentagon is bent inwards along the thick line. If we choose exactly the right value of d as shown in the middle, we get a flat pentagon.

On the other hand, for any value of d we can flatten out the pentagon and lay it out in the plane.

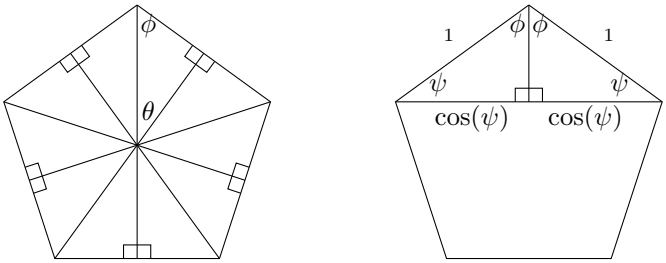


If d is too small or too large then the pentagon will not be regular. The miraculous thing is that the value of d that makes the pentagon flat is the same value that makes it regular; our next task is to prove this.

Lemma 8.2. *In the regular pentagon with sides of length* 1*, the distance* τ *in the diagram below satisfies* $\tau = 2\cos(\pi/5) = (1+\sqrt{5})/2$*, and moreover we have* $1/(\tau-1) = \tau$*.*



Proof. We can divide the pentagon into right angled triangles as shown on the left below. All the angles in the middle are equal to θ and there are ten of them so $\theta = 2\pi/10 = \pi/5$. As the angles of any triangle add up to π, we have $\phi = \pi/2 - \theta = 3\pi/10$.



Now consider the picture on the right, which shows that $\tau = 2\cos(\psi)$. We have a triangle with angles $\pi/2$, ϕ and ψ so $\psi = \pi - \pi/2 - \phi = \pi/2 - \phi = \theta = \pi/5$, so we conclude that $\tau = 2\cos(\pi/5)$.

We next claim that $\tau^2 - \tau - 1 = 0$. To see this, put $\xi = e^{\pi i/5} = \cos(\pi/5) + i\sin(\pi/5)$, so $\xi^{-1} = e^{-\pi i/5} = \cos(\pi/5) - i\sin(\pi/5)$, so $\xi + \xi^{-1} = 2\cos(\pi/5) = \tau$. We find that

$$\begin{aligned}\tau^2 - \tau - 1 &= (\xi^2 + 2 + \xi^{-2}) - (\xi + \xi^{-1}) - 1 \\ &= \xi^2 - \xi + 1 - \xi^{-1} + \xi^{-2},\end{aligned}$$

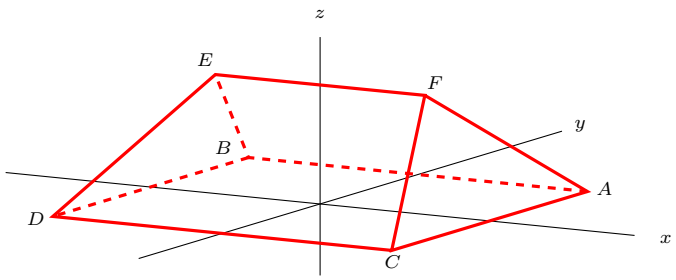
so

$$\begin{aligned}(1+\xi)(\tau^2-\tau-1) &= (1+\xi)(\xi^2-\xi+1-\xi^{-1}+\xi^{-2})\\ &= \xi^3+\xi^{-2} = \xi^{-2}(\xi^5+1).\end{aligned}$$

However, we also have $\xi^5 = e^{i\pi} = -1$, so $\xi^5+1=0$, so $(1+\xi)(\tau^2-\tau-1)=0$. As $\xi \neq -1$ we can divide by ξ to deduce that $\tau^2-\tau-1=0$ as claimed.

Solving this equation gives $\tau = (1\pm\sqrt{5})/2$, but $(1-\sqrt{5})/2 < 0$ and τ is clearly positive so we must have $\tau = (1+\sqrt{5})/2$. We can also rearrange the equation $\tau^2-\tau-1=0$ as $(\tau-1)\tau = 1$ and so $1/(\tau-1)=\tau$. □

Now let T be a tent whose base is a square of side τ and whose other edges have length 1. We place T with its base in the xy-plane parallel to the axes with the centre of the base at the origin and with the ridge parallel to the x-axis.



It should be clear that the coordinates of $A,\dots,D$ are as follows:

$$\begin{aligned} A &= (\tau/2,\tau/2,0) & B &= (-\tau/2,\tau/2,0)\\ C &= (\tau/2,-\tau/2,0) & D &= (-\tau/2,-\tau/2,0)\end{aligned}$$

Moreover, the line EF is horizontal and lies in the xz plane and it crosses the z-axis at its midpoint. This means that the y coordinates of E and F are zero, their z-coordinates are the same, and the x coordinate of E is minus the x coordinate of F. Thus for some a,b we have $E=(-a,0,b)$ and $F=(a,0,b)$.

Next, recall that the edges FA, FC, EB, ED and EF have length 1. As $\vec{EF} = (2a,0,0)$ and EF has length 1 we must have $a = 1/2$. Thus

$$\begin{aligned}\vec{FA} = A-F &= (\tau/2-a,\tau/2,-b)\\ &= ((\tau-1)/2,\tau/2,-b)\\ &= ((\sqrt{5}-1)/4,(\sqrt{5}+1)/4,-b).\end{aligned}$$

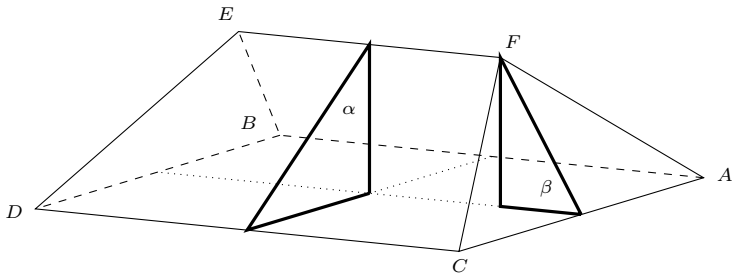
As FA has length 1 we conclude that

$$\begin{aligned}1 &= (\sqrt{5}-1)^2/16+(\sqrt{5}+1)^2/16+(-b)^2\\ &= (6-2\sqrt{5})/16+(6+2\sqrt{5})/16+b^2\\ &= 3/4+b^2.\end{aligned}$$

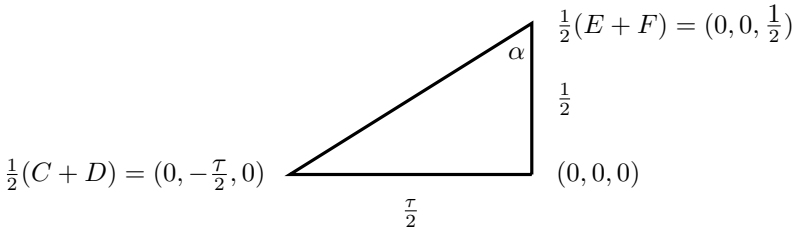
This gives $b^2 = 1/4$ so $b = 1/2$. In summary, we have

$$\begin{aligned} A &= (\tau/2,\tau/2,0) & B &= (-\tau/2,\tau/2,0)\\ C &= (\tau/2,-\tau/2,0) & D &= (-\tau/2,-\tau/2,0)\\ E &= (-1/2,0,1/2) & F &= (1/2,0,1/2).\end{aligned}$$

Lemma 8.3. *The angles α and β indicated below are the same.*

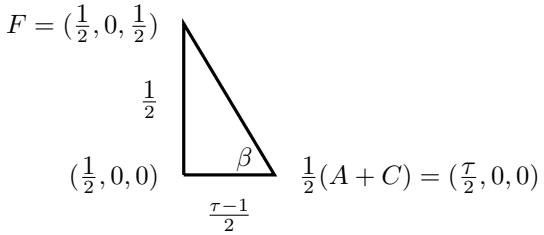


Proof. The left hand triangle looks like this.



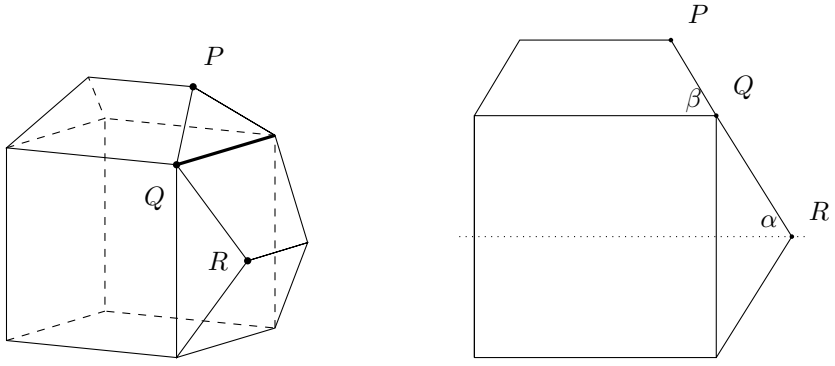
The top vertex is the midpoint of EF which is $\frac{1}{2}(E+F)$ and using our formulae for E and F we see that this is just $(0, 0, \frac{1}{2})$. The bottom right vertex is in the xy-plane directly underneath $(0, 0, \frac{1}{2})$, so it must be $(0, 0, 0)$. The bottom left vertex is the midpoint of CD, which is $\frac{1}{2}(C+D) = (0, -\frac{\tau}{2}, 0)$. It follows easily that the sides have length $\frac{1}{2}$ and $\frac{\tau}{2}$ as shown, and thus that $\tan(\alpha) = \frac{\tau}{2}/\frac{1}{2} = \tau$.

In a similar way, we see that the right hand triangle is as follows:



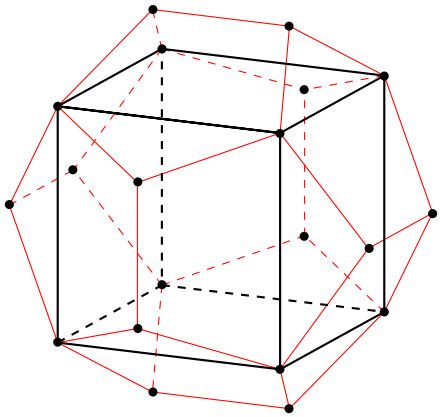
This shows that $\frac{\tan(\beta)=\frac{1}{2}/\tau-1}{2=1/(\tau-1)}$. We know from Lemma 8.2 that $1/(\tau-1) = \tau$ so $\tan(\beta) = \tan(\alpha)$ so $\beta = \alpha$. □

Now suppose we attach two tents to a cube of side τ as shown on the left.



Looking from the side we see the picture on the right. As $\alpha = \beta$ we see that P, Q and R lie on a straight line, so the pentagon is flat as required.

We now attach a tent to each face, giving the following picture.



The same argument as before shows that all the pentagons are flat. You can just now just look at the picture to see that we have twelve regular pentagonal faces, as required.

Proposition 8.4. *The dodecahedron has* 20 *vertices and* 30 *edges.*

Proof. There are 12 faces each with 5 edges, apparently giving $5 \times 12 = 60$ edges. However, each edge is an edge of two different faces, so we have counted each edge twice; there are really only $60/2 = 30$ edges. Similarly, there are 12 faces each with 5 vertices, but each vertex occurs on three different faces, so there are $12 \times 5/3 = 20$ vertices altogether. □

9. Symmetries of the dodecahedron

We now investigate the group $G := \mathrm{Dir}(\mathrm{Dodec})$ of direct symmetries of the dodecahedron.

If g is a symmetry of the cube, it may or may not move the tents around in such a way as to preserve the dodecahedron. For example, if we do a quarter around the z-axis then the ridge of the top tent ends up at right angles to the way it originally was, so the dodecahedron is not preserved. However, a half turn about the z-axis (or the x-axis or y-axis) does send tents to tents and thus gives a symmetry of the dodecahedron. These half twists are given by the matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad , \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

These matrices commute and have order two, and the product of any two of them is the third one. It follows that together with the identity they form a group of order four.

Next, if we do a one-third twist about a long diagonal of the cube we get another symmetry of the dodecahedron, this time of order 3.

Finally, if we let L be the line joining the centres of two opposite faces then a rotation through $2\pi/5$ also preserves the dodecahedron. It would take some work to prove this from our construction, but I hope that it is reasonably clear geometrically.

Proposition 9.1. *The group* $G = \mathrm{Dir}(\mathrm{Dodec})$ *has order* 60*, and it is generated by the rotations of order* 2*,* 3 *and* 5 *mentioned above.*

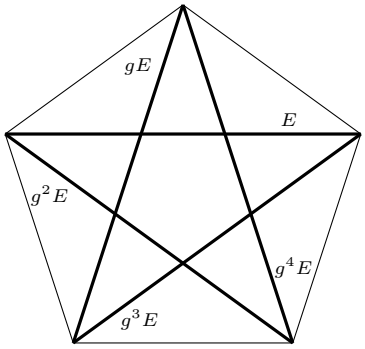
Proof. Let H be the subgroup of G generated by the rotations considered previously. We have seen that H has a subgroup of order 4 and that it contains an element of order 3 and an element of order 5. It follows that $|H|$ is divisible by 4, 3 and 5. As these numbers are coprime, it follows that $|H|$ is divisible by $4 \times 3 \times 5 = 60$. As H is a subgroup of G, we see that $|G|$ is divisible by $|H|$ and thus is divisible by 60.

Now let G act on the vertices of the dodecahedron, and choose a vertex v. The orbit-stabiliser theorem says that $|G|$ is the the order of the orbit Gv times the order of the stabiliser group $\mathrm{stab}_G(v)$. There are 20 vertices, so $|Gv| \leq 20$. If $g \in \mathrm{stab}_G(v)$ then g must be a rotation around v, and by looking at the three edges meeting at v we see that the only possible angles are 0 and $\pm 2\pi/3$. This shows that $|\mathrm{stab}_G(v)| = 3$ and thus that $|G| = |Gv||\mathrm{stab}_G(v)| \leq 20 \times 3 = 60$. As $|H| \leq |G| \leq 60$ and $|H|$ is divisible by 60 we must have $|G| = |H| = 60$ and $G = H$. □

Theorem 9.2. *G is isomorphic to A_5.*

Proof. Let D denote the dodecahedron. By construction, D contains an inscribed cube C, and each face of D is cut across by a single edge of C. If $g \in G$ then gC is a cube inscribed in D, and is typically different from C. Let X be the set of all the cubes that arise in this way. The group G acts on the set X, and by construction the orbit of of the element $C \in X$ is the whole of X. Thus, the orbit-stabiliser theorem says that $|G| = |X||K|$, where K is the stabiliser of C. In other words, K is the set of rotations that preserve both the cube C and the dodecahedron D, so K is a subgroup of $\mathrm{Dir}(C)$. It follows that $24 = |\mathrm{Dir}(C)|$ is divisible by $|K|$. However, K is not equal to $\mathrm{Dir}(C)$ (because a quarter-twist around the z-axis does not preserve D) so $|K| < 24$. On the other hand, K contains the group of order 4 generated by half-twists around the axes and it also contains elements of order 3 given by rotating around the long diagonals, so $|K|$ is divisible by 12. It follows that $|K|$ must be equal to 12. As $|G| = |X||K|$ and $|G| = 60$ and $|K| = 12$ we have $X = 5$.

Another way to see that X has five elements is as follows. Choose a face F of D, and let E be the edge of C that cuts across F. Let g be a rotation through $2\pi/5$ around the centre of F, so $g^k F = F$ for $k = 0, \dots, 4$. Then $g^k E$ is the edge of $g^k C$ that cuts across F. As the edges $g^k E$ are all different (for $k = 0, 1, 2, 3, 4$), the cubes $g^k C$ must all be different, so we have at least five cubes.

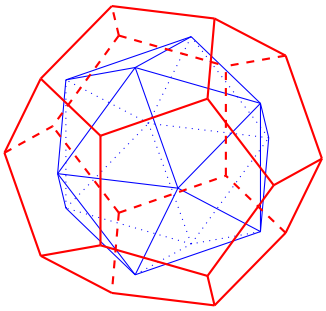
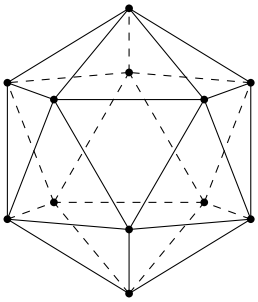


It is a bit more difficult to show that there are *exactly* five cubes by this method.

The action of G on X gives a homomorphism $\phi\colon G \to S_5$. If g is as above then $\phi(g)$ is clearly a 5-cycle, and thus an even permutation. If h is a one-third twist about a vertex of C, then $\phi(h)^3 = \phi(h^3) = 1$, so $\phi(h)$ is a permutation of $\{1, \dots, 5\}$ of order dividing 3. One checks that the only possibilities are the identity and the 3-cycles, and by inspecting a model we see that $\phi(h)$ is not the identity so it must be a 3-cycle. In particular, it is again an even permutation. Now let k_x, k_y and k_z be the half-twists about the x, y and z-axes. By inspecting a model again we see that $\phi(k_x)$, $\phi(k_y)$ and $\phi(k_z)$ are distinct elements of S_5 of the form $(a\ b)(c\ d)$, so they are again even permutations. It follows that $\{1, \phi(k_x), \phi(k_y), \phi(k_z)\}$ is a subgroup of A_5 of order 4. As elements of the three types just considered generate G, we see that $\phi(x)$ is an even permutation for all $x \in G$, so $\phi(G) \leq A_5$. We have also seen that $\phi(G)$ contains a group of order 4 and elements of orders 3 and 5, so $|\phi(G)|$ is divisible by $3 \times 4 \times 5 = 60$. However, we also have $|A_5| = 5!/2 = 60$, so we must have $\phi(G) = A_5$. Thus $\phi\colon G \to A_5$ is a surjective map between two sets that both have exactly 60 elements, so ϕ must be a bijection. Thus ϕ gives an isomorphism $G \simeq A_5$ as claimed. □

10. The icosahedron

The icosahedron is the dual of the dodecahedron. We'll write D for the dodecahedron and I for the icosahedron. The centres of the 12 faces of D are the 12 vertices of I. If v is a vertex of D, then 3 faces of D (say F_1, F_2 and F_3) meet at v. If we write w_i for the centre of F_i then w_1, w_2 and w_3 are vertices of I, and they form an equilateral triangle which is a face of I. This gives 20 faces, one for each of the 20 vertices of D.

The picture on the left shows I inside D. The picture on the right shows I rotated into a more natural position.

11. Finite subgroups of SO_3

We now consider the classification of finite subgroups of SO_3. We have already met the groups

$$G_1 = \mathrm{Dir}(\mathrm{Tet}) \simeq A_4 \qquad |G_1| = 12$$
$$G_2 = \mathrm{Dir}(\mathrm{Cube}) = \mathrm{Dir}(\mathrm{Oct}) \simeq S_4 \qquad |G_2| = 24$$
$$G_3 = \mathrm{Dir}(\mathrm{Dodec}) = \mathrm{Dir}(\mathrm{Icos}) \simeq A_5 \qquad |G_3| = 60.$$

The orders of these groups are 12, 24 and 60.

Now let n be any natural number. Let $\widetilde{R}$ be a rotation through $2\pi/n$ around the z-axis, anticlockwise as seen from above. This clearly has order n so the set $\widetilde{C}_n = \{1, \widetilde{R}, \dots, \widetilde{R}^{n-1}\}$ is a subgroup of SO_3 which is cyclic of order n. Strictly speaking this is different from C_n but it is usually harmless to ignore the distinction.

Now let $\widetilde{S}$ be a half-turn around the x-axis. Note that the effect of $\widetilde{S}$ on the xy-plane is the same as a reflection across the x-axis. One can easily check that $\widetilde{S}^2 = 1$ and $\widetilde{S}\widetilde{R}\widetilde{S} = \widetilde{R}^{-1}$ and that the set

$$\widetilde{D}_n = \{1, \widetilde{R}, \dots, \widetilde{R}^{n-1}, \widetilde{S}, \widetilde{R}\widetilde{S}, \dots, \widetilde{R}^{n-1}\widetilde{S}\}$$

is a subgroup of SO_3 of order $2n$. Again, it is usually harmless to identify this with D_n.

Another point of view is as follows. Given a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in O_2$, define

$$\lambda(A) = \left(\begin{array}{cc|c} a & b & 0 \\ c & d & 0 \\ \hline 0 & 0 & 1/\det(A) \end{array}\right).$$

It is not hard to check that λ is a homomorphism and that $\lambda(R_{2\pi/n}) = \widetilde{R}$ and $\lambda(S_0) = \widetilde{S}$, so $\widetilde{C}_n = \lambda(C_n)$ and $\widetilde{D}_n = \lambda(D_n)$.

The classification theorem is as follows.

Theorem 11.1. *Let G be a finite subgroup of SO_3. Then G is conjugate to one of the groups G_1, G_2, G_3, $\widetilde{C}_n$ or $\widetilde{D}_n$ (for some n).*

The rest of this section will constitute the proof.

Definition 11.2. If $g \in SO_3 \setminus \{1\}$ (so g is a nontrivial rotation of $\mathbb{R}^3$) then the *poles* of g are the two unit vectors on the axis of rotation of g, or in other words the two unit vectors v such that $g(v) = v$. If G is a finite subgroup of SO_3, the poles of G are the poles of all the elements $g \in G$ such that $g \neq 1$.

Remark 11.3. A unit vector v is a pole of G iff $g(v) = v$ for some $g \in G$ with $g \neq 1$, iff the group $\mathrm{stab}_G(v) = \{g \in G \mid g(v) = v\}$ is not the trivial group.

Remark 11.4. Often it is natural to describe a rotation g as being a rotation around w for some non-unit vector w. We will write $\hat{w} = w/\|w\|$, which is a positive multiple of w and is a unit vector. We call this the *normalisation* of w. Clearly g is also a rotation around $\hat{w}$.

Remark 11.5. Let v be any unit vector. Rotations around v are determined by their angles in just the same way that rotations of the plane are determined by their angles. Thus, we can analyse the finite groups of rotations around v in the same way that we analysed the finite subgroups of SO_2; we find that they are all cyclic. In particular, if v is a pole of G we find that $\text{stab}_G(v)$ is a nontrivial finite group of rotations about v, so it is cyclic of order d for some $d > 1$. We call d the *degree* of v.

Definition 11.6. From now on we fix a finite subgroup $G \leq SO_3$, and we let P be the set of poles of G. We write $n = |G|$ and $p = |P|$.

Lemma 11.7. *The action of G on $\mathbb{R}^3$ preserves the set P.*

Proof. Suppose that $v \in P$ and $h \in G$; we must show that $h(v) \in P$. As $v \in P$ there is some nontrivial element $g \in G$ with $g(v) = v$. Thus $g' := hgh^{-1}$ is another nontrivial element of g and $g'(h(v)) = hgh^{-1}h(v) = hg(v) = h(v)$. Thus $h(v)$ is a pole of g' and thus lies in P, as required. □

Our main technique will be to study the orbits of the action of G on P. As a warm-up we consider the case where there are only two poles.

Theorem 11.8. *If G is a finite subgroup of SO_3 and the set P of poles has order 2 then G is cyclic.*

Proof. Choose $v \in P$. Clearly $-v \in P$ also, and as $|P| = 2$ we must have $P = \{v, -v\}$. Given $g \in G \setminus \{1\}$, we know that g is a rotation about some axis L, and we choose a unit vector w on L. Clearly w is a pole of G, so $w \in P = \{v, -v\}$, so $v = w$ or $v = -w$. Either way we see that $gv = v$; thus v is fixed under G. Now let U be the plane perpendicular to v. If $u \in U$ then $\langle gu, v\rangle = \langle gu, gv\rangle = \langle u, v\rangle = 0$, so $gu \in U$ also. Thus, G is a finite subgroup of the group of rotations of the plane U, which is isomorphic to SO_2. We know from Proposition 2.3 that a finite subgroup of SO_2 is cyclic, so G is cyclic. □

We next record how the orbits work for the groups we already know about.

(a) The nontrivial elements of the group $G_1 = \text{Dir(Tet)}$ are the rotations through $\pm 2\pi/3$ about the vertices of the tetrahedron and the rotations through π about the midpoints of the edges. Let $v_1, \dots, v_4$ be the vertices, so the two unit vectors on the line through v_i are $\pm\hat{v}_i$. If $i < j$ then there is an edge joining v_i to v_j, whose midpoint is $v_{ij} := (v_i + v_j)/2$. We thus have

$$\begin{aligned} P = \{&\hat{v}_1, \hat{v}_2, \hat{v}_3, \hat{v}_4, \\ &-\hat{v}_1, -\hat{v}_2, -\hat{v}_3, -\hat{v}_4, \\ &\hat{v}_{12}, \hat{v}_{13}, \hat{v}_{14}, \hat{v}_{23}, \hat{v}_{24}, \hat{v}_{34}\}. \end{aligned}$$

You might think that we should include $-\hat{v}_{12}$ (for example) but in fact it is there already. The centre of the tetrahedron is $(v_1 + v_2 + v_3 + v_4)/4$ but this is just the origin, so $-(v_1 + v_2) = v_3 + v_4$. It follows that $-\hat{v}_{12} = \hat{v}_{34}$, which is already in the list. Similarly, for any $i < j$ we can let k and l be the other two numbers in the range $\{1, 2, 3, 4\}$ and we have $-\hat{v}_{ij} = \hat{v}_{kl}$.

It is not hard to see that we can send any vertex of Tet to any other vertex by the action of G_1, so the set $\{v_1, v_2, v_3, v_4\}$ is an orbit of the action. This implies that $\{-v_1, -v_2, -v_3, -v_4\}$ is also an orbit. Similarly, as we can send any edge to any other edge by the action of G_1, we see that $\{\hat{v}_{12}, \hat{v}_{13}, \hat{v}_{14}, \hat{v}_{23}, \hat{v}_{24}, \hat{v}_{34}\}$ is another orbit. Thus there are two orbits of poles of degree 3 and one orbit of poles of degree 2, making three orbits altogether.

(b) The nontrivial elements of the group $G_2 = \text{Dir(Cube)}$ are:
- rotations through π about midpoints of edges of the cube
- rotations through $\pm 2\pi/3$ about vertices
- rotations through π or $\pm\pi/2$ about centres of faces.

Here the negative of the midpoint of an edge is the midpoint of the opposite edge, the negative of a vertex is the opposite vertex, and the negative of the centre of a face is the centre of the opposite face. Thus, we do not need to worry about negatives, and the poles are the normalisations of midpoints of edges, vertices, and centres of faces. There are 12 edges, 8 vertices and 6 faces so we have $12 + 8 + 6 = 26$ poles altogether. As we can move any edge to any other edge by the action of G_2, we see that the first 12 poles form an orbit. As we can move any vertex to any other vertex, we see that the next 8 poles form an orbit. As we can move any face to any other face, we see that

the last 6 poles form an orbit. Thus we have one orbit consisting of 12 poles of degree 2, one orbit consisting of 8 poles of degree 3, and one orbit consisting of 6 poles of degree 4. Again we have 3 orbits altogether.

(c) The nontrivial elements of $G_3 = \mathrm{Dir}(\mathrm{Dodec})$ are:
- rotations through π about midpoints of edges of the dodecahedron
- rotations through $\pm 2\pi/3$ about vertices
- rotations through $\pm 2\pi/5$ or $\pm 4\pi/5$ about centres of faces.

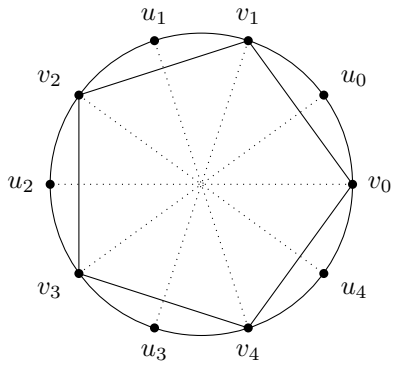
Just as in the case of the cube, we do not have to worry about negatives. There are 30 edges, 20 vertices and 12 faces. We thus have one orbit consisting of 30 poles of degree 2, one orbit consisting of 20 poles of degree 3, and one orbit consisting of 12 poles of degree 5.

(d) Now consider the cyclic group $\widetilde{C}_n$. All the nontrivial elements are rotations around the unit vector $w = (0, 0, 1)$, so $P = \{w, -w\}$. All elements of the group send w to w and $-w$ to $-w$, so $\{w\}$ and $\{-w\}$ are two separate orbits. There are thus 2 orbits, each consisting of 1 pole of degree n.

(e) Finally, consider the dihedral group $\widetilde{D}_n$. The poles of the elements R^i (for $i = 1, \dots, n-1$) are just w and $-w$ again. Now consider the points

$$v_k = (\cos(2k\pi/n), \sin(2k\pi/n), 0)$$
$$u_k = (\cos((2k+1)\pi/n), \sin((2k+1)\pi/n), 0).$$

These are defined for all $k \in \mathbb{Z}$ but $v_{k+n} = v_k$ and $u_{k+n} = u_k$ so there are really only n v's and n u's. We show the case $n = 5$ below.



It is geometrically clear that a half twist around v_k or u_k preserves the standard n-gon X_n and thus lies in $\widetilde{D}_n$, so the u's and v's are poles of $\widetilde{D}_n$. We also need to think about the points $-u_i$ and $-v_j$. When n is odd (as in the above picture) we see that $-u_i = v_k$ for some k and $-v_j = u_l$ for some l. If n is even we see instead that $-u_i$ has the form u_k and $-v_j$ has the form v_l. Either way, we get no new poles. Also, any symmetry of X_n sends vertices to vertices, and we can move any vertex to any other vertex, so the v's form an orbit. Similarly, the u's form an orbit. Thus, the u's and v's give 2 orbits, each consisting of n poles of degree 2. Moreover, we have $R^k(w) = w$ and $S(w) = -w$ so $\{w, -w\}$ is an orbit consisting of 2 poles of degree n. Thus we again have three orbits altogether.

We now let G be an arbitrary finite subgroup of SO_3. Our next task is to show that the number of poles and orbits for G matches one of the possibilities discussed above. Our main tool is the orbit counting theorem:

Theorem 11.9. *Let H be a finite group that acts on a finite set X. For each $h \in H$ put $\mathrm{Fix}(h) = \{x \in X \mid hx = x\}$, the set of fixed points of h. Then the number of orbits of H in X is $|H|^{-1} \sum_{h \in H} |\mathrm{Fix}(h)|$, or in other words the average number of fixed points of an element of H.* □

Proposition 11.10. *Let G be a nontrivial finite subgroup of SO_3, and let P be the set of poles of G. Put $n = |G|$ and $p = |P|$, and let m be the number of orbits of G in P. Let d_k be the degree of the poles in the*

k'th orbit; we can order the orbits in such a way that $d_1 \leq d_2 \leq \ldots \leq d_m$. Then

$$m = (p + 2n - 2)/n$$
$$p = \sum_{k=1}^{m} n/d_k.$$

Proof. The orbit counting theorem says that $m = n^{-1} \sum_{g \in G} |\operatorname{Fix}(g)|$. If $g \neq 1$ then $\operatorname{Fix}(g)$ consists of the two unit vectors on the axis of g, so $|\operatorname{Fix}(g)| = 2$. There are $n - 1$ elements $g \in G$ with $g \neq 1$, so $\sum_{g \neq 1} |\operatorname{Fix}(g)| = 2(n-1) = 2n - 2$. In the remaining case $g = 1$ we have $\operatorname{Fix}(g) = P$ and thus $|\operatorname{Fix}(g)| = p$. This means that $\sum_{g \in G} |\operatorname{Fix}(g)| = p + 2n - 2$ and thus $m = (p + 2n - 2)/n$.

Next, choose a point x_k in the k'th orbit for each k. Then $\operatorname{stab}_G(x_k)$ has order d_k. The orbit-stabiliser theorem says that $|G| = |\operatorname{stab}_G(x_k)||\operatorname{orb}_G(x_k)|$, so the size of the k'th orbit is $|G|/|\operatorname{stab}_G(x_k)| = n/d_k$. As P is the disjoint union of the orbits we see that $p = |P|$ is the sum of the orders of all the orbits, so $p = \sum_k n/d_k$, as claimed. □

Proposition 11.11. *With notation as above we have either*

(1) *$m = 3$, $d_1 = 2$, $d_2 = d_3 = 3$ and $n = 12$; or*
(2) *$m = 3$, $d_1 = 2$, $d_2 = 3$, $d_3 = 4$ and $n = 24$; or*
(3) *$m = 3$, $d_1 = 2$, $d_2 = 3$, $d_3 = 5$ and $n = 60$; or*
(4) *$m = p = 2$ and $d_1 = d_2 = n$; or*
(5) *there is an integer $d \geq 2$ such that $m = 3$, $n = 2d$, $d_1 = d_2 = 2$ and $d_3 = d$.*

Proof. First note that d_k is the order of the stabiliser group of x_k. As x_k is a pole, this stabiliser group is nontrivial, so $d_k \geq 2$.

Next, we can rearrange the equation $m = (p + 2n - 2)/n$ as $m = 2 + (p-2)/n$. By assumption G is a nontrivial group, and any nontrivial element has two poles, so $p \geq 2$, which implies that $(p-2)/n \geq 0$ and $m \geq 2$.

Alternatively, we can rearrange to get $p = mn - 2n + 2$. We also know that $p = \sum_{k=1}^{m} n/d_k$. As each d_k is at least 2, each term in the on the right hand side is at most $n/2$, and there are m terms, so $p \leq mn/2$. After feeding this back into the equation $p = mn - 2n + 2$ we find that $mn/2 \leq 2n - 2 < 2n$ so $mn < 4n$ so $m < 4$. As $m \geq 2$ and $m < 4$ we must have $m = 2$ or $m = 3$.

If $m = 2$ then the equation $m = 2 + (p-2)/2$ implies that $p = 2$. The equation $p = \sum_k n/d_k$ now says that $2 = n/d_1 + n/d_2$. As d_k divides n for all k the terms n/d_1 and n/d_2 are positive integers, so the only way their sum can be 2 is if $n/d_1 = n/d_2 = 1$, so $d_1 = d_2 = n$, so case (4) holds.

Now suppose instead that $m = 3$. The equation $m = 2 + (p-2)/n$ then simplifies to give $p = n + 2$, and we can feed this into the equation $p = \sum n/d_k = n/d_1 + n/d_2 + n/d_3$ and rearrange to give

$$\frac{2}{n} = \frac{1}{d_1} + \frac{1}{d_2} + \frac{1}{d_3} - 1.$$

Recall that $2 \leq d_1 \leq d_2 \leq d_3$. If the d's are reasonably large then $1/d_1$, $1/d_2$ and $1/d_3$ will be small and so $1/d_1 + 1/d_2 + 1/d_3 - 1$ will be negative, which is absurd because $2/n$ is certainly positive. Thus, the d's must be fairly small. We can complete the proof by making this argument more precise.

We first claim that $d_1 = 2$. Indeed, if not then $3 \leq d_1 \leq d_2 \leq d_3$, so $1/d_1$, $1/d_2$ and $1/d_3$ are all less than or equal to $1/3$ so $1/d_1 + 1/d_2 + 1/d_3 - 1 \leq 3/3 - 1 = 0$, which contradicts the equation $2/n = (\sum 1/d_k) - 1$.

We thus have $d_1 = 2$ as claimed. Suppose we also have $d_2 = 2$. Then $2/n = 1/2 + 1/2 + 1/d_3 - 1 = 1/d_3$, so $n = 2d_3$. We are thus in case (5).

Now suppose instead that $d_2 > 2$. We claim that in fact $d_2 = 3$. Indeed, if not then $4 \leq d_2 \leq d_3$ so $1/d_2$ and $1/d_3$ are at most $1/4$, so $1/d_1 + 1/d_2 + 1/d_3 - 1 \leq 1/2 + 1/4 + 1/4 - 1 = 0$, which contradicts the equation $2/n = (\sum 1/d_k) - 1$.

We thus have $d_1 = 2$ and $d_2 = 3$ and $d_3 \geq 3$, so $2/n = 1/2 + 1/3 + 1/d_3 - 1 = 1/d_3 - 1/6$. If $d_3 = 3$ this gives $2/n = 1/3 - 1/6 = 1/6$ so $n = 12$ and we are in case (1). If $d_3 = 4$ then $2/n = 1/4 - 1/6 = 1/12$ so $n = 24$ and we are in case (2). If $d_3 = 5$ then $2/n = 1/5 - 1/6 = 1/30$ so $n = 60$ and we are in case (3). If $d_3 \geq 6$ then $2/n = 1/d_3 - 1/6 \leq 0$, which is absurd. □

Proposition 11.12. *If case (1) holds in Proposition 11.11 then G is conjugate to $G_1 = \operatorname{Dir}(\mathrm{Tet})$.*

Proof. Let V be the third orbit, which has order $n/d_3 = 12/3 = 4$, so $V = \{v_1, v_2, v_3, v_4\}$ say. Let g be a one-third turn around v_4, which lies in G because v_4 is a pole of degree 3. Clearly g gives a permutation of $\{v_1, v_2, v_3\}$. The only way that a one-third turn can permute a set of three points is if they form an equilateral triangle perpendicular to the axis of rotation, with the centre of the triangle on the axis. It follows that the distances $d(v_1, v_4)$, $d(v_2, v_4)$ and $d(v_3, v_4)$ are all the same. Similarly, by rotating around v_3 we see that $d(v_1, v_3) = d(v_2, v_3) = d(v_4, v_3)$. We can also rotate around v_1 or v_2 and we find that all the distances $d(v_i, v_j)$ (for $i \neq j$) are the same. This means that v_1, v_2, v_3 and v_4 are the vertices of a regular tetrahedron T. As G permutes these vertices, it is a subgroup of $\mathrm{Dir}(T)$, but $|G| = 12 = |\mathrm{Dir}(T)|$ so $G = \mathrm{Dir}(T)$. Let r be the distance from the origin to the vertices of the standard tetrahedron Tet, and put $T' = rT$; it is not hard to see that $\mathrm{Dir}(T') = \mathrm{Dir}(T) = G$. As T' is a regular tetrahedron the same size as Tet, we can choose an isometry $f \in SO_3$ with $f(\mathrm{Tet}) = T'$. It follows that

$$\mathrm{Dir}(T') = \mathrm{Dir}(f(\mathrm{Tet})) = f\,\mathrm{Dir}(\mathrm{Tet})f^{-1} = fG_1f^{-1},$$

so G is conjugate to G_1. □

Proposition 11.13. *If case (2) holds in Proposition 11.11 then G is conjugate to $G_2 = \mathrm{Dir}(\mathrm{Oct})$.*

Proof. Let V be the third orbit, which has order $n/d_3 = 24/4 = 6$. If $v \in V$ then v is a pole of degree 4 so $-v$ is also a pole of degree 4. The poles in the other two orbits have degree 2 or 3, so we must have $-v \in V$. It follows that V has the form $\{v_1, v_2, v_3, -v_1, -v_2, -v_3\}$ for some v_1, v_2 and v_3. Let g be a quarter turn around v_3, which lies in G because v_3 is a pole of degree 4. Clearly $g(v_3) = v_3$ and $g(-v_3) = -v_3$ so g must permute the remaining vertices $\{v_1, v_2, -v_1, -v_2\}$. The only way that a quarter turn can permute a set of four points is if they form a square perpendicular to the axis of rotation. It follows that the distances $d(v_3, v_1)$, $d(v_3, v_2)$, $d(v_3, -v_1)$ and $d(v_3, -v_2)$ are all the same, equal to r say. We also have

$$d(-v_3, v_1) = \|v_1 - (-v_3)\| = \|v_3 + v_1\| = \|v_3 - (-v_1)\| = d(v_3, -v_1) = r,$$

and by the same method we find that $d(-v_3, -v_1) = d(-v_3, v_2) = d(-v_3, -v_2) = r$. We can also rotate about v_1 or v_2 instead, and we find that

$$d(\pm v_1, \pm v_2) = d(\pm v_1, \pm v_3) = d(\pm v_2, \pm v_1) = d(\pm v_2, \pm v_3) = r.$$

Using this, we find that the points in V are the vertices of a regular octahedron O, so $G \leq \mathrm{Dir}(O)$, but $|G| = 24 = |\mathrm{Dir}(O)|$ so $G = \mathrm{Dir}(O)$. By the same method as in the previous proposition we find that G is conjugate to G_2. □

Proposition 11.14. *If case (3) holds in Proposition 11.11 then G is conjugate to $G_3 = \mathrm{Dir}(\mathrm{Icos})$.*

Proof. Let V be the third orbit, which has order $n/d_3 = 60/5 = 12$. We will show that the points in V are the vertices of an icosahedron.

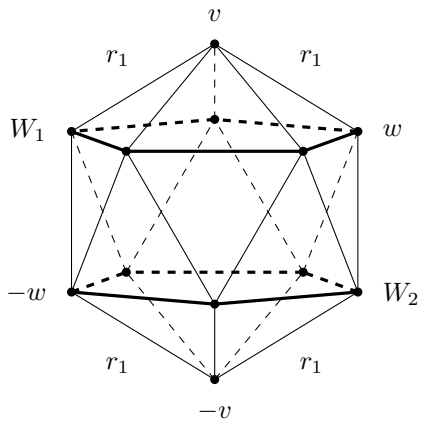
If $v \in V$ then v is a pole of degree 5 so $-v$ is also a pole of degree 5. The poles in the other two orbits have degree 2 or 3, so we must have $-v \in V$. Put $V' = V \setminus \{v, -v\}$ so $|V'| = 10$, let g be a one-fifth turn around v, and let H be the subgroup of order 5 generated by g. We see geometrically that for any $x \in \mathbb{R}^3$ that does not lie on the axis of g, the orbit Hx has order 5. None of the points in V' lie on the axis, so V' must split into two orbits of order 5 under the action of H, say $V' = W_1 \cup W_2$. All the points in W_1 lie at the same distance (say r_1) from v, and all the points in W_2 lie at some other distance r_2 from v. We may assume that $r_1 \leq r_2$ (otherwise rename W_1 as W_2 and W_2 as W_1). We will actually assume that $r_1 < r_2$; one can check by going through the following argument more carefully that the equation $r_1 = r_2$ leads to a contradiction.

Now let u be any point in V. As V is an orbit there exists an element $h \in G$ with $hv = u$. For any point $w' \in W_1$ we then have $d(u, hw') = d(hv, hw') = d(v, w') = r_1$. Thus all the points in hW_1 lie at distance r_1 from u, and similarly the points in hW_2 lie at distance r_2. This means that u has 5 nearest neighbours, and they all lie at distance r_1 from u.

Choose a point $w \in W_1$. I claim that $-w \in W_2$. Indeed, $-w$ is certainly a pole of degree 5 and $-w \neq \pm v$ so $-w \in V' = W_1 \cup W_2$. It will thus be enough to show that $-w \notin W_1$. If $-w \in W_1$ we have $-w = g^k w$ for some k, which means that $-w = (-1)^5 w = g^{5k} w = w$ (because $g^5 = 1$). This means that $w = 0$, which is impossible as w is a unit vector. We must therefore have $-w \in W_2$ as required. Note that

$d(-v,-w) = d(v,w) = r_1$ and $d(-v,w) = d(v,-w) = r_2$, so all the points in W_2 lie at distance r_1 from $-w$ and all the points in W_1 lie at distance r_2 from $-w$.

We thus have a picture like this. The points in W_1 are the vertices of the top pentagon, and the points in W_2 are the vertices of the bottom pentagon.



Because the nearest neighbours of any vertex lie at distance r_1 from that vertex, we see that all the edges have length r_1 so we have a regular icosahedron, which we call I. Clearly $G \leq \mathrm{Dir}(I)$ but $|G| = 60 = |\mathrm{Dir}(I)|$, so $G = \mathrm{Dir}(I)$. It follows as usual that G is conjugate to G_3. □

Proposition 11.15. *If case (4) holds in Proposition 11.11 then G is conjugate to $\widetilde{C}_n$.*

Proof. This is essentially Theorem 11.8. □

Proposition 11.16. *If case (5) holds in Proposition 11.11 and $d > 2$ then G is conjugate to $\widetilde{D}_d$.*

Proof. Let P_1, P_2 and P_3 be the three orbits in P. Choose w in P_3, so w has degree d. Then $-w$ also has degree d and the poles in the first two orbits have degree 2 so $-w \in P_3$. We also have $|P_3| = n/d_3 = 2d/d = 2$, so $P_3 = \{w, -w\}$. Let g be the rotation through $2\pi/d$ around w, and let U be the plane through the origin perpendicular to w.

Now suppose that $v \in P_2$, and let h be the half turn around v, which lies in G because v is a pole of degree 2. As P_3 is an orbit we have $hP_3 = P_3$ so $hw = \pm w$. The only way that a half twist around v can send w to $-w$ is if v is perpendicular to w. Thus all the points in P_2 lie in the plane U, and similarly all the points in P_1 lie in U.

Note also that the points $v, gv, \dots, g^{d-1}v$ are all different and all lie in P_2, and $|P_2| = n/d_2 = 2d/2 = d$, so we must have $P_2 = \{v, gv, \dots, g^{d-1}v\}$. We can choose coordinate so that $w = (0,0,1)$ and $v = (1,0,0)$. Then U is the xy-plane and P_2 consists of the vertices of the standard polygon X_d, with polar coordinates $[1, 2k\pi/d]$.

By a similar argument, the set P_1 consists of d equally spaced points on the unit circle in the xy-plane, and these points are all different from the points $g^k v$. Thus there must be precisely one of the the points in P_1 lying in the gap between v and gv; call this point u. Let α be the angle between u and v, and let β be the angle between u and gv. The half twist around u must send P_2 to itself, and clearly this can only happen if v and gv are exchanged, and this means that $\alpha = \beta$. As $\alpha + \beta$ is the angle between v and gv, which is $2\pi/d$, we have $\alpha = \beta = \pi/d$. We also have $P_1 = \{u, gu, \dots, g^{d-1}u\}$, which is the set of points with polar coordinates $[1, (2k+1)\pi/d]$. The group G consists of the rotations g^k together with the half-twists around the points in P_1 and P_2, so $G = \widetilde{D}_d$. This refers to $\widetilde{D}_d$ as defined with respect to our new coordinate system: if $\widetilde{D}_d$ is defined using the original coordinate system, then G is merely conjugate to $\widetilde{D}_d$. □

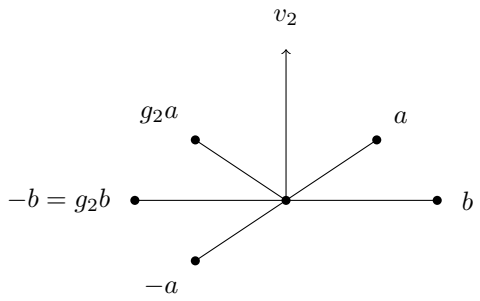
Proposition 11.17. *If case (5) holds in Proposition 11.11 and $d = 2$ then G is conjugate to $\widetilde{D}_2$.*

Proof. In this case we have $m = 3$, $d_1 = d_2 = d_3 = 2$ and $|G| = n = 4$. Let P_i be the i'th orbit, so $|P_i| = n/d_i = 2$, so $P_i = \{v_i, w_i\}$, say. Let g_i be a half twist around v_i, which lies in G because $d_i = 2$. Note

that every element of G sends $P_i = \{v_i, w_i\}$ to itself and g_i sends v_i to v_i so it must send w_i to w_i. Thus, w_i is a fixed point of g_i and the only two fixed points are v_i and $-v_i$ so we must have $w_i = -v_i$.

Now consider $g_2 v_1$. As the orbit of v_1 is $\{v_1, -v_1\}$ we must have $g_2 v_1 = \pm v_1$ and v_1 is not one of the fixed points of g_2 so we must have $g_2 v_1 = -v_1$.

You should be able to see from the following picture that $g_2 b = -b$ if and only if b is perpendicular to v_2.



As $g_2 v_1 = -v_1$, the vectors v_1 and v_2 must be orthogonal to each other. By a similar argument, they are both orthogonal to v_3. Thus G consists of the identity together with half twists around three orthogonal axes, whereas $\widetilde{D}_2$ consists of the identity together with half-twists about the standard x, y and z-axes. It follows that G is conjugate to $\widetilde{D}_2$. □

12. The Sylow theorems

Let G be a finite group of order n, say. Lagrange's theorem says that if H is a subgroup of G and $|H| = d$, then d is a divisor of n. It is natural to ask whether the converse is true: given a divisor d of n, can we find a subgroup $H \leq G$ such that $|H| = d$? The answer is no in general; for example one can check that the group A_4 has order 12 but there is no subgroup of order 6. However, if d is a power of a prime number, then the answer turns out to be yes, and in fact we can say a great deal more. This follows from the Sylow theorems, which we will prove in this section.

Fix a finite group G and a prime p. We can write $|G|$ in the form $p^v m$, where p does not divide m. A *Sylow p-subgroup* of G is a subgroup $P \leq G$ such that $|P| = p^v$. We write n_p for the number of Sylow p-subgroups of G (which *a priori* could be zero).

Theorem 12.1. (a) *There is at least one Sylow p-subgroup, so $n_p > 0$.*
(b) *Moreover, n_p divides m and is congruent to 1 mod p.*
(c) *Any two Sylow p-subgroups are conjugate.*
(d) *Any p-subgroup of G is contained in a Sylow p-subgroup.*

Before giving the proof, we outline some applications. These will be discussed in more detail and extended in the next section.

Example 12.2. Let G be a group of order $35 = 5 \times 7$. Then n_5 divides 7 so $n_5 = 1$ or $n_5 = 7$, but also $n_5 = 1 \pmod 5$ so we must have $n_5 = 1$. Thus, there is precisely one subgroup $P \leq G$ with $|P| = 5$. Moreover, we know that n_7 divides 5 and $n_7 = 1 \pmod 7$ so $n_7 = 1$, so there is a unique subgroup $Q \leq G$ of order 7. Using the fact that P is unique we see that it is normal in G; this will be explained in Proposition 12.5 below. Similarly, Q is normal. The order of $P \cap Q$ divides $|P| = 5$ and also divides $|Q| = 7$, so $|P \cap Q| = 1$ so $P \cap Q = \{1\}$. Using this and the fact that P and Q are normal and $|G| = |P||Q|$ one can check that $G \simeq P \times Q \simeq C_5 \times C_7$. Thus, any group of order 35 is isomorphic to $C_5 \times C_7$.

Example 12.3. Recall that a group G is *simple* if the only normal subgroups of G are $\{1\}$ and G. Let G be a simple group of order 60. We'll outline a proof that G must be isomorphic to A_5. Note that $60 = 2^2 \times 15$ so n_2 divides 15 by part (b) of the Theorem, so $n_2 \in \{1, 3, 5, 15\}$. If $n_2 = 1$ then the unique Sylow 2-subgroup is normal, contradicting the simplicity of G. A slightly more complicated argument shows that n_2 cannot be 3 either. Indeed, G acts by conjugation on the set of Sylow 2-subgroups, giving a homomorphism $\phi\colon G \to S_{n_2}$. This is nontrivial, because all Sylow 2-subgroups are conjugate, by part (c) of the Theorem. This means that $\ker(\phi) \neq G$ and $\ker(\phi)$ is a normal subgroup of G so we must have $\ker(\phi) = \{1\}$. This means that ϕ

is injective, so $|G| \leq |S_{n_2}|$, so $n_2! \geq 60$. As $4! = 24$ and $5! = 120$ the equation $n_2! \geq 60$ is equivalent to $n_2 \geq 5$. We already know that $n_2 \in \{1, 3, 5, 15\}$ so $n_2 = 5$ or $n_2 = 15$. In fact the case $n_2 = 15$ cannot occur (although we will not prove this here) so $n_2 = 5$. We thus have an injective homomorphism $\phi\colon G \to S_5$. As ϕ is injective, the image $\phi(G)$ has order 60, and one can check that A_5 is the only subgroup of S_5 of order 60, so ϕ gives an isomorphism $G \simeq A_5$.

Proof of (a). Let $\mathcal{X}$ be the set of all subsets $X \subseteq G$ such that $|X| = p^v$. In general, any set of order N has $\left(\begin{array}{c} N \\ M \end{array}\right)$ subsets of order M, so $|\mathcal{X}| = \left(\begin{array}{c} p^v m \\ p^v \end{array}\right)$. We claim that this number is not divisible by p. To see this, put $q = p^v m - p^v = p^v(m-1)$ and note that $\left(\begin{array}{c} p^v m \\ p^v \end{array}\right) = (p^v m)!/(p^v!\, q!)$. We also have

$$(p^v m)!/q! = (q+1)(q+2)\dots(q+p^v)$$

so

$$\left(\begin{array}{c} p^v m \\ p^v \end{array}\right) = \frac{1}{q+1}\frac{2}{q+2}\cdots\frac{p^v}{q+p^v} = \prod_{j=1}^{p^v}\frac{j}{q+j}.$$

Now let w_j be the largest number such that j is divisible by p^{w_j} (for $j = 1, \dots, p^v$). As $j \leq p^v$ we must have $w_j \leq v$ so the number $q = p^v(m-1)$ is also divisible by p^{w_j}. It follows that $q + j$ is divisible by p^{w_j} as well, so all the p's on the top in our equation for $\left(\begin{array}{c} p^v m \\ p^v \end{array}\right)$ are cancelled out by p's on the bottom. It follows that $|\mathcal{X}| \neq 0 \pmod p$, as claimed.

Now let G act on $\mathcal{X}$ by $gX = \{gx \mid x \in X\}$, and divide $\mathcal{X}$ into orbits under this action, say $\mathcal{X} = \mathcal{X}_1 \cup \dots \cup \mathcal{X}_k$. Orbits are always disjoint so $|\mathcal{X}| = \sum_j |\mathcal{X}_j|$. If each of the numbers $|\mathcal{X}_j|$ were divisible by p, then $|\mathcal{X}|$ would also be divisible by p, contrary to what we just proved. Thus we can choose j such that the number $m' := |\mathcal{X}_j|$ is not divisible by p. Choose an element $X \in \mathcal{X}_j$, so (by the definition of $\mathcal{X}$) X is a subset of G with p^v elements. Put $P = \operatorname{stab}_G(X) = \{g \in G \mid gX = X\}$. The orbit-stabiliser theorem says that $|G| = |\operatorname{stab}_G(X)||\operatorname{orb}_G(X)|$, or in other words $p^v m = |P|m'$. As p^v divides $|P|m'$ and p does not divide m' we see that p^v divides $|P|$. Next, fix an element $x_0 \in X$. For each $g \in P$ we have $gx_0 \in gX = X$ so $Px_0 \subseteq X$, so $p^v = |X| \geq |Px_0| = |P|$. As p^v divides $|P|$ and $|P| \leq p^v$ we must have $|P| = p^v$, so P is a Sylow p-subgroup of G. □

For the remaining parts we need the following lemma. Recall that a *p-group* is a group whose order is a power of the prime p.

Lemma 12.4. *Let P be a finite p-group, and let X be a set with an action of P. Put*

$$\operatorname{Fix}(P) = \operatorname{Fix}(P, X) = \{x \in X \mid gx = x \text{ for all } g \in P\}.$$

Then $|\operatorname{Fix}(P)| = |X| \pmod p$. In particular, if $|X| \neq 0 \pmod p$ then $\operatorname{Fix}(P) \neq \emptyset$.

Proof. The order of P is p^v for some $v \geq 0$. Divide X into orbits and list them in order of size, say $X = X_1 \cup \dots \cup X_k$ with $|X_1| \leq |X_2| \leq \dots \leq |X_k|$. As each set X_j is an orbit, its order divides $|P| = p^v$, so $|X_j| = p^{w_j}$ for some w_j with $0 \leq w_1 \leq w_2 \leq \dots \leq w_k \leq v$. For some r (possibly $r = 0$) we have $w_j = 0$ when $1 \leq j \leq r$ and $w_j > 0$ when $j > r$. We have

$$|X| = \sum_{j=1}^{k} |X_j| = \sum_{j=1}^{r} 1 + \sum_{j=r+1}^{k} p^{w_j} = r + \sum_{j>r} p^{w_j} = r \pmod p.$$

On the other hand, an eement $x \in X$ lies in $\operatorname{Fix}(P)$ if and only if the orbit Px consists of the single element x, so $|\operatorname{Fix}(P)|$ is the number of orbits of size 1, which is r. Thus $|X| = |\operatorname{Fix}(P)| \pmod p$, as claimed.

Now suppose that $|X| \neq 0 \pmod p$. Then $|\operatorname{Fix}(P)| \neq 0 \pmod p$, so $|\operatorname{Fix}(P)| \neq 0$, so $\operatorname{Fix}(X) \neq \emptyset$. □

Proof of (c) and (d). Let P be a Sylow p-subgroup of G, and let Q be any p-subgroup of G. Note that $|P| = p^v$ and $|Q| = p^w$ for some $w \leq v$. As usual we write G/P for the set of right cosets of P, so a typical element of G/P has the form xP for some $x \in G$. Note that $|G/P| = |G|/|P| = m$, which is not divisible by p. We let Q act on G/P by $g*(xP) = gxP$ for $g \in Q$. Note that $|G/P| = m \neq 0 \pmod p$ and Q is a p-group so by Lemma 12.4 there is a fixed point, in other words a coset xP such that $gxP = xP$ for all $g \in Q$. This

means that $x^{-1}gxP = P$, so $x^{-1}gx \in P$, so $g = x(x^{-1}gx)x^{-1} \in xPx^{-1}$. This proves that $Q \subseteq xPx^{-1}$. Now xPx^{-1} is conjugate to P so it is a subgroup of G with the same order as P, in other words it is another Sylow p-subgroup. This shows that Q is contained in a Sylow p-subgroup, as claimed in (d).

Now suppose that Q itself is a Sylow p-subgroup. Then $Q \leq xPx^{-1}$ but $|Q| = |xPx^{-1}| = p^v$ so $Q = xPx^{-1}$. Thus Q is conjugate to P, as claimed in (c). □

Proof of (b). Let $\mathcal{P}$ be the set of all Sylow p-subgroups of G, so $n_p = |\mathcal{P}|$. Let G act on $\mathcal{P}$ by conjugation, so $g * P = gPg^{-1}$. Choose a Sylow p-subgroup $P \in \mathcal{P}$, and put

$$N = \operatorname{stab}_G(P) = \{g \in G \mid gPg^{-1} = P\}.$$

It is clear that $P \leq N \leq G$ so p^v divides $|N|$ and $|N|$ divides $p^v m$, so $|N| = p^v k$ for some k dividing m.

As all Sylow p-subgroups are conjugate to P, we have $\mathcal{P} = \operatorname{orb}_G(P)$ and so $|G| = |N||\mathcal{P}|$, so $p^v m = p^v k n_p$, so $m = kn_p$. Thus n_p divides m.

Note also that P can be thought of as a Sylow p-subgroup of N. Part (c) of the Theorem works for any finite group, in particular it works for the group N, so any other Sylow p-subgroup Q of N is conjugate *in* N to P. This means that $Q = gPg^{-1}$ for some $g \in N$. By the definition of N, this means that $Q = P$. Thus, P is the *unique* Sylow p-subgroup of N.

Before we considered the action of all of G on $\mathcal{P}$; now we restrict attention to the action of the subgroup P. Lemma 12.4 tells us that $|\operatorname{Fix}(P, \mathcal{P})| = |\mathcal{P}| = n_p \pmod p$. We want to prove that $n_p = 1 \pmod p$, so it will be enough to show that $\operatorname{Fix}(P, \mathcal{P}) = \{P\}$. Clearly if $g \in P$ then $gPg^{-1} = P$, which shows that $P \in \operatorname{Fix}(P, \mathcal{P})$. Conversely, suppose that $Q \in \operatorname{Fix}(P, \mathcal{P})$, so Q is a Sylow p-subgroup and $gPg^{-1} = P$ for all $g \in Q$. This means that Q is a Sylow p-subgroup of N, which means that $Q = P$ by the previous paragraph. Thus $\operatorname{Fix}(P, \mathcal{P}) = \{P\}$ and $|\operatorname{Fix}(P, \mathcal{P})| = 1$ as required. □

Proposition 12.5. *If $n_p = 1$ then the Sylow p-subgroup of G is a normal subgroup. If $n_p > 1$ then none of the Sylow p-subgroups is normal.*

Proof. Suppose that $n_p = 1$, so there is a unique Sylow p-subgroup, which we call P. If $g \in G$ then gPg^{-1} is a Sylow p-subgroup so it must be equal to P; this says that P is normal.

Now suppose that $n_p > 1$. If P is any Sylow p-subgroup, we can choose a different Sylow p-subgroup, say Q. As all such subgroups are conjugate, there is some $g \in G$ such that $gPg^{-1} = Q \neq P$. This means that P is not normal. □

13. Groups of small order

We now try to classify groups of various small orders, using the Sylow theorems as one of our main tools. Many of our results involve the cyclic groups:

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

with $R^n = 1$. We start with two general facts about these groups.

Lemma 13.1. *If G is a group and $g \in G$ and $g^n = 1$, then there is a homomorphism $\phi\colon C_n \to G$ with $\phi(R) = g$.*

Proof. As $C_n = \{1 = R^0, R, \dots, R^{n-1}\}$, we can define a function $\phi\colon C_n \to G$ by $\phi(R^i) = g^i$ for $i = 0, \dots, n-1$. To see that this is a homomorphism, consider two elements $R^i, R^j \in C_n$ with $0 \leq i < n$. If $i + j < n$ then

$$\phi(R^i.R^j) = \phi(R^{i+j}) = g^{i+j} = g^i g^j = \phi(R^i)\phi(R^j).$$

Suppose instead that $i + j \geq n$. By assumption we have $0 \leq i, j < n$, so $i + j < 2n$. Thus, if we put $k = i + j - n$ then $0 \leq k < n$, so $\phi(R^k) = g^k$. We also have

$$R^i R^j = R^{i+j} = R^{k-n} = R^k (R^n)^{-1} = R^k$$
$$g^i g^j = g^{i+j} = g^{k-n} = g^k (g^n)^{-1} = g^k$$

so

$$\phi(R^i.R^j) = \phi(R^{i+j}) = \phi(R^k) = g^k = g^i g^j = \phi(R^i)\phi(R^j).$$

We thus have $\phi(R^i.R^j) = \phi(R^i)\phi(R^j)$ in all cases, showing that ϕ is a homomorphism. □

Lemma 13.2. *If n and m are coprime, then $C_{nm} \simeq C_n \times C_m$.*

Proof. We write r_k for the generator of C_k, and define $\phi\colon C_{nm} \to C_n \times C_m$ by $\phi(r_{nm}^i) = (r_n^i, r_m^i)$. It is easy to see that this is a homomorphism. Suppose that r_{nm}^i lies in the kernel of ϕ. This means that $(r_n^i, r_m^i) = (1, 1)$, which means that $r_n^i = 1$ in C_n and $r_m^i = 1$ in C_m. As $r_n^i = 1$ we see that i must be divisible by n, and as $r_m^i = 1$ we see that i must be divisible by m. As n and m are coprime this means that i is divisible by nm, so $r_{nm}^i = 1$. This shows that the kernel of ϕ is the trivial group, so ϕ is injective. This means that $|\phi(C_{nm})| = |C_{nm}| = nm = |C_n \times C_m$, so $\phi(C_{nm})$ must be all of $C_n \times C_m$, so ϕ is surjective as well as injective, so ϕ is an isomorphism. □

We next recall the basic result about groups of prime order.

Proposition 13.3. *If G is a group whose order is a prime number p, then G is isomorphic to C_p.*

Proof. Let g be any element of G other than the identity. Then the order of g is not equal to 1 and it divides p so it must be equal to p. The subgroup generated by g is thus equal to the whole group, and it follows that G is cyclic of order p. More precisely, we can define a homomorphism $\phi\colon C_p \to G$ by $\phi(R^i) = g^i$, and we find that ϕ is an isomorphism. □

We would next like to study groups of order p^2, where p is prime. We will first need a result about general p-groups.

Definition 13.4. The *centre* of a group G is the set $Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$, so an element z lies in the centre if and only if it commutes with all other elements. One checks that $Z(G)$ is a normal subgroup of G and that it is Abelian.

Example 13.5. The centre of the symmetric group S_n is the trivial group (provided that $n > 2$). To see this, suppose that σ lies in the centre. For each i, let ρ_i be the $(n-1)$-cycle formed by the numbers $1, \dots, n$ with i missing, so $\rho_i(i) = i$ and $\rho_i(j) \neq j$ if $j \neq i$. Now $\rho_i\sigma = \sigma\rho_i$ so $\rho_i(\sigma(i)) = \sigma(\rho_i(i)) = \sigma(i)$, so $\sigma(i)$ is fixed by the action of ρ_i. The only fixed point is i, so $\sigma(i) = i$. This holds for all i, so $\sigma = 1$.

Proposition 13.6. *If P is a nontrivial p-group then $Z(P) \neq \{1\}$.*

Proof. Let P act on itself by conjugation, so $g * x = gxg^{-1}$. Note that $g * x = x$ if and only if $gx = xg$, or in other words g commutes with x. Thus x is fixed under the action of P iff $g * x = x$ for all g, iff $x \in Z(P)$. Thus Lemma 12.4 tells us that $|Z(P)| = |P| \pmod p$. As P is a nontrivial p-group we have $|P| = p^v$ for some $v > 0$ so $|P| = 0 \pmod p$, so $|Z(P)|$ is divisible by p. Moreover, $1 \in Z(P)$ so $|Z(P)| > 0$. It follows that $|Z(G)| \geq p$, so $Z(G) \neq \{1\}$. □

Lemma 13.7. *Let G be a finite group, and let P and Q be subgroups of G. Define a function $\phi\colon P \times Q \to G$ by $\phi(x, y) = xy$.*

(a) *If every element of P commutes with every element of Q, then ϕ is a homomorphism.*
(b) *If we also have $P \cap Q = \{1\}$, then ϕ is injective.*

Proof. (a) Suppose that every element of P commutes with every element of Q. Consider elements $x_0, x_1 \in P$ and $y_0, y_1 \in Q$, so (x_0, y_0) and (x_1, y_1) are elements of $P \times Q$. We then have

$$\begin{aligned}
\phi((x_0, y_0)(x_1, y_1)) &= \phi((x_0x_1, y_0y_1)) && \text{(definition of } P \times Q) \\
&= x_0x_1y_0y_1 && \text{(definition of } \phi) \\
&= x_0y_0x_1y_1 && \text{(because } x_1 \text{ commutes with } y_0) \\
&= \phi((x_0, y_0))\phi((x_1, y_1)) && \text{(definition of } \phi)
\end{aligned}$$

This shows that ϕ is a homomorphism.

(b) Now suppose as well that $P \cap Q = \{1\}$. Consider an element $(x, y) \in \ker(\phi)$. This means that $(x, y) \in P \times Q$ and and $\phi((x, y)) = 1$, or in other words, $x \in P$ and $y \in Q$ and $xy = 1$. This means that $x = y^{-1}$, and $y \in Q$, so $x \in Q$. We are also given that $x \in P$, so $x \in P \cap Q = \{1\}$, so $x = 1$. This means that $y^{-1} = 1$, so $y = 1$, so $(x, y) = (1, 1)$. This proves that the kernel of ϕ is the trivial group, so ϕ is injective.

□

Proposition 13.8. *Let G be a group of order p^2. Then G is isomorphic either to $C_p \times C_p$ or to C_{p^2} (and so G is always Abelian).*

Proof. If G has an element of order p^2 then it is cyclic and thus isomorphic to C_{p^2}. Suppose instead that all nontrivial elements of G have order p. By Proposition 13.6, we can choose a nontrivial element $z \in Z(G)$. This generates a subgroup $P \leq Z(G) \leq G$ of order p. Let g be any element of G not lying in P, and let Q be the subgroup generated by g, which again has order p. By Lemma 13.7, we can define a homomorphism $\phi\colon P \times Q \to G$ by $\phi(x, y) = xy$. Let H be the image of ϕ, so H is a subgroup of G, so $|H|$ divides $|G| = p^2$, so $|H|$ is 1, p or p^2. It is clear that $P \leq H$ and $g \in H \setminus P$, so $|H| \geq p + 1$, so $|H|$ must be p^2. This means that $H = G$, so ϕ is surjective. As $P \times Q$ and G have the same size, any sutrjective function between them must be bijective, so ϕ is an isomorphism. We also know that P and Q are both isomorphic to C_p, so $G \simeq P \times Q \simeq C_p \times C_p$. □

Proposition 13.9. *Let G be a finite group, and let P and Q be* normal *subgroups of orders p and q. Suppose that p and q are coprime, and that $pq = |G|$. Then $G \simeq P \times Q$.*

Proof. First, put $r = |P \cap Q|$. As $P \cap Q$ is a subgroup of P, we see that r divides p. As $P \cap Q$ is a subgroup of Q, we see that r also divides q. As p and q are coprime, this means that $r = 1$, so $P \cap Q$ is the trivial group.

Now consider elements $x \in P$ and $y \in Q$, and put $z = xyx^{-1}y^{-1}$. We will show that $z \in P \cap Q$, so that $z = 1$. Indeed, we have $y \in Q$ and Q is normal, so $xyx^{-1} \in Q$. As y^{-1} also lies in Q, we deduce that $z = (xyx^{-1})y^{-1} \in Q$. Similarly, we know that $x^{-1} \in P$ and P is normal so $yx^{-1}y^{-1} \in P$. We also know that $x \in P$, so $z = x(yx^{-1}y^{-1}) \in P$. This gives $z \in P \cap Q$, so $z = 1$, or in other words $1 = xyx^{-1}y^{-1}$. If we multiply this on the right by yx, we get $yx = xyx^{-1}y^{-1}yx = xy$, so x commutes with y. Lemma 13.7 now tells us that we can define an injective homomorphism $\phi\colon P \times Q \to G$ by $\phi(x, y) = xy$. As this is injective, we have

$$|\phi(P \times Q)| = |P \times Q| = pq = |G|,$$

so $\phi(P \times Q) = G$, so ϕ is also surjective. This means that ϕ is an isomorphism of groups. □

Proposition 13.10. *Let G be a group of order pq where p and q are primes and $p < q$. Suppose also that $q - 1$ is not divisible by p. Then $G \simeq C_p \times C_q$.*

Proof. We know that n_p divides q and q is prime so $n_p = 1$ or $n_p = q$. However we also know that $n_p = 1 \pmod p$ so p divides $n_p - 1$. We are told that p does not divide $q - 1$, so n_p cannot be equal to q, so $n_p = 1$. It follows that there is a unique Sylow p-subgroup, which we call P. Note that $|P| = p$ and so $P \simeq C_p$, and also that P is normal.

Next, we know that n_q divides p, so $n_q = 1$ or $n_q = p$. We also know that $n_q = 1 \pmod q$, so $n_q - 1$ is divisible by q. Note that $0 < p - 1 < q$, so $p - 1$ cannot be divisible by q, so we must have $n_q = 1$. We therefore have a unique Sylow q-subgroup, which we call Q. We note that $|Q| = q$ and that Q is normal.

It is now clear that the conditions of Proposition 13.9 are satisfied, so $G \simeq P \times Q \simeq C_p \times C_q$. □

Proposition 13.11. *Let p be a prime number with $p > 2$, and let G be a group with $|G| = 2p$. Then either $G \simeq C_p \times C_2 \simeq C_{2p}$ or $G \simeq D_p$.*

Proof. We know that n_p divides 2 and that $n_p - 1$ is divisible by p. It follows that $n_p = 1$, so there is a unique Sylow p-subgroup, which we call P. We choose a nontrivial element $g \in P$, and define an isomorphism $\phi\colon C_p \to P$ by $\phi(R^i) = g^i$.

Next, let Q be a Sylow 2-subgroup, so $|Q| = 2$, so $Q = \{1, h\}$ for some element h with $h^2 = 1$. As P is normal, we know that $hgh^{-1} \in P$, so $hgh^{-1} = g^a$ for some a. It follows that

$$h^2gh^{-2} = hg^ah^{-1} = (hgh^{-1})^a = (g^a)^a = g^{(a^2)}.$$

On the other hand, we have $h^2 = 1$, so $h^{-2} = 1$, so $h^2gh^{-2} = g$. We thus have $g = g^{a^2}$, so $g^{a^2-1} = 1$, so $a^2 - 1$ must be divisible by p. As p is prime and $a^2 - 1 = (a + 1)(a - 1)$, we see that either $a + 1$ or $a - 1$ must be divisible by p.

If $a - 1$ is divisible by p then $g^a = g$, so $h^{-1}gh = g$, so g commutes with h. In this case, the conditions of Lemma 13.7 are satisfied and we find that $G \simeq P \times Q \simeq C_p \times C_2 \simeq C_{2p}$.

Suppose instead that $a+1$ is divisible by p. This means that $g^a = g^{-1}$, so $hgh^{-1} = g^{-1}$. We then define a function $\phi\colon D_p \to G$ by $\phi(R^i) = g^i$ and $\phi(R^iS) = g^ih$ for $0 \leq i < p$. It is straightforward to check that this is a homomorphism, the key point being that $SRS^{-1} = R^{-1}$ in D_p, which corresponds to the relation $hgh^{-1} = g^{-1}$ in G. The image of ϕ contains both P and Q, so the order of the image is divisible by p and 2 and thus by $2p$. It follows that ϕ is surjective, but the groups D_p and G have the same order, so ϕ must actually be an isomorphism. □

Remark 13.12. The above proposition can be extended to show that when p and q are distinct primes, any group of order pq is a "semidirect product" of C_p and C_q.

Now consider groups of order at most 40. Using Propositions 13.3, 13.8, 13.10 and 13.11, we can classify all groups of the following orders:

$$1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 15, 17, 19, 22, 23, 25, 26, 29, 31, 33, 35, 37, 38.$$

More work is needed to classify groups of the remaining orders:

$$8, 12, 16, 18, 20, 21, 24, 27, 28, 32, 34, 36, 39.$$

14. Automorphisms and semidirect products

Definition 14.1. An *automorphism* of a group G is an isomorphism from G to itself. We write $\mathrm{Aut}(G)$ for the set of all automorphisms of G. This set is itself a group under composition.

Example 14.2. Consider the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Define $\sigma\colon G \to G$ by $\sigma(x, y) = (y, x)$. Clearly $\sigma^2(x, y) = \sigma(y, x) = (x, y)$ so σ^2 is the identity map so σ is an inverse for itself. This means that σ is a bijection. Also

$$\sigma((v, w) + (x, y)) = \sigma(v + x, w + y) = (w + y, v + x) = (w, v) + (y, x) = \sigma(v, w) + \sigma(x, y),$$

which proves that σ is a homomorphism and thus is an automorphism of G. In othe words, σ is an element of the group $\mathrm{Aut}(G)$. We can define another homomorphism $\rho\colon G \to G$ by $\rho(x, y) = (y, x+y)$. We then have $\rho^2(x, y) = \rho(y, x+y) = (x+y, y+(x+y)) = (x+y, x)$ and $\rho^3(x, y) = \rho(x+y, x) = (x, x+(x+y)) = (x, y)$, so $\rho^3 = 1$, so ρ is an automorphism. One can check that

$$\mathrm{Aut}(G) = \{1, \rho, \rho^2, \sigma, \rho\sigma, \rho^2\sigma\}$$

and using this that $\mathrm{Aut}(G) \simeq D_3$.

Proposition 14.3. *If G is cyclic of order n then $\mathrm{Aut}(G) \simeq \mathbb{Z}_n^\times$.*

Proof. Suppose $a \in \mathbb{Z}_n$. If $x \in G$ then $x^n = 1$ so the powers of x depend only on the exponent modulo n, so it makes sense to talk about x^a. We define a function $\alpha_a\colon G \to G$ by $\alpha_a(x) = x^a$. Because G is cyclic it is Abelian and this implies that $(xy)^a = x^a y^a$ or in other words $\alpha_a(xy) = \alpha_a(x)\alpha_a(y)$, so α_a is a homomorphism. Clearly also $\alpha_a\alpha_b(x) = \alpha_a(x^b) = (x^a)^b = x^{ab} = \alpha_{ab}(x)$, so $\alpha_a\alpha_b = \alpha_{ab}$. Similarly $\alpha_1(x) = x$, so α_1 is the identity map, and $\alpha_0(x) = 1$, so α_0 is the trivial homomorphism.

We next claim that every homomorphism $\beta\colon G \to G$ has the form $\beta = \alpha_a$ for a unique element $a \in \mathbb{Z}_n$. Indeed, we can choose a generator $g \in G$ so that $G = \{1, g, \dots, g^{n-1}\} = \{g^a \mid a \in \mathbb{Z}_n\}$. We then have $\beta(g) \in G$ so $\beta(g) = g^a$ for a unique element $a \in \mathbb{Z}_n$. As β is a homomorphism we have

$$\beta(g^i) = \beta(g)^i = (g^a)^i = g^{ia} = \alpha_a(g^i)$$

for all i, so $\beta = \alpha_a$.

Now, if $a \in \mathbb{Z}_n^\times$ then a has an inverse $b \in \mathbb{Z}_n^\times$ and then $\alpha_a\alpha_b = \alpha_{ab} = \alpha_1 = 1$ and similarly $\alpha_b\alpha_a = 1$ so α_b is an inverse for α_a. This means that α_a is an automorphism of G, in other words $\alpha_a \in \mathrm{Aut}(G)$.

Conversely, suppose that β is an automorphism of G. Then β and β^{-1} are homomorphisms from G to itself, say $\beta = \alpha_a$ and $\beta^{-1} = \alpha_b$ for some $a, b \in \mathbb{Z}_n$. We then have $\alpha_{ab} = \beta\beta^{-1} = 1 = \alpha_1$, so $ab = 1$, so $a \in \mathbb{Z}_n^\times$. This shows that the automorphisms of G are precisely the maps α_a with $a \in \mathbb{Z}_n^\times$.

We can now define a map $\phi\colon \mathbb{Z}_n^\times \to \mathrm{Aut}(G)$ by $\phi(a) = \alpha_a$, and we find that this is an isomorphism. □

Construction 14.4. *Suppose that G is a group and N is a normal subgroup. For any $g \in G$ we know that $N = gNg^{-1}$. We can therefore define $\gamma_g\colon N \to N$ by $\gamma_g(x) = gxg^{-1}$. This is a homomorphism because*

$$\gamma_g(x)\gamma_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = \gamma_g(xy).$$

We also have

$$\gamma_g(\gamma_h(x)) = \gamma_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \gamma_{gh}(x),$$

so $\gamma_g\gamma_h = \gamma_{gh}$. In particular, this means that $\gamma_{g^{-1}}$ is an inverse for γ_g, so γ_g is an automorphism of N, in other words $\gamma_g \in \mathrm{Aut}(N)$.

Construction 14.5. *Now suppose that G is a semidirect product of N and Q. We define a function $\phi\colon Q \to \mathrm{Aut}(N)$ by $\phi(g) = \gamma_g$. We then have $\phi(g)\phi(h) = \gamma_g\gamma_h = \gamma_{gh} = \phi(gh)$, so ϕ is a homomorphism.*

Example 14.6. Consider the group $G = \mathbb{Z}_n \rtimes_a \mathbb{Z}_m$ as the semidirect product of $N = \{(v, 0) \mid v \in \mathbb{Z}_n\}$ and $Q = \{(0, w) \mid w \in \mathbb{Z}_m\}$. We then have $\mathrm{Aut}(N) \simeq \mathbb{Z}_n^\times$ and $Q \simeq \mathbb{Z}_m$. We also have

$$\gamma_{(0,w)}(v, 0) = (0, w)(v, 0)(0, -w) = (a^w v, w)(0, -w) = (a^w v, 0).$$

This means that the automorphism $\gamma_{(0,w)} \in \mathrm{Aut}(N)$ corresonds to the element $a^w \in \mathbb{Z}_n^\times$ and that the homomorphism $\phi\colon \mathbb{Z}_m \to \mathbb{Z}_n^\times$ is given by $\phi(w) = a^w$.

Proposition 14.7. *If G is a semidirect product as above and $\phi\colon Q \to \mathrm{Aut}(N)$ is the trivial homomorphism then every element of Q commutes with every element of N and $G \simeq N \times Q$.*

Proof. If ϕ is trivial then for each $g \in Q$, the homomorphism $\phi(g) = \gamma_g\colon N \to N$ is the identity map, in other words $\gamma_g(x) = x$ for all $x \in N$. As $\gamma_g(x) = gxg^{-1}$ this means that $gxg^{-1} = x$ so $gx = xg$ so g commutes with x.

Now define $\mu\colon N \times Q \to G$ by $\mu(x, g) = xg$. We claim that this is a homomorphism. Recall that the group structure in $N \times Q$ is just given by $(x, g)(y, h) = (xy, gh)$, so we must show that $\mu(x, g)\mu(y, h) = \mu(xy, gh)$ or in other words that $xgyh = xygh$. This is true because g commutes with y.

As G is a semidirect product of N and Q, we have $NQ = G$ and $N \cap Q = \{1\}$. As $NQ = G$ we see that μ is surjective. If $(x, g) \in \ker(\mu)$ then $xg = 1$ so $g = x^{-1}$. Now $g \in Q$ and $x^{-1} \in N$ so the element $g = x^{-1}$ lies in $N \cap Q = \{1\}$ so $g = x = 1$. Thus $\ker(\mu) = \{(1, 1)\}$, which shows that μ is injective and thus an isomorphism. □