PROBLEMS ON GROUPS AND SYMMETRY

N. P. STRICKLAND

Exercise 1. Note that $R_\pi(x) = -x$. Give expressions for $R_{a,\pi}(x)$, $R_{a,\pi}^{-1}(x)$ and $R_{a,\pi}R_{b,\pi}R_{a,\pi}^{-1}R_{b,\pi}^{-1}(x)$. Check that your last answer is consistent with the formula in the notes for $R_{a,\theta}R_{b,\phi}R_{a,\theta}^{-1}R_{b,\phi}^{-1}$.

Solution: First, we have $R_{a,\pi} = T_a R_\pi T_{-a}$, so $R_{a,\pi}(x) = a + R_\pi(x-a) = a-(x-a) = 2a-x$. If $y = 2a-x$ then $x = 2a-y$; this shows that $R_{a,\pi}^{-1}(y) = 2a-y$ and thus $R_{a,\pi}^{-1} = R_{a,\pi}$. Using this we have

$$\begin{aligned} R_{a,\pi}R_{b,\pi}R_{a,\pi}^{-1}R_{b,\pi}^{-1}(x) &= 2a-(2b-(2a-(2b-x))) \\ &= 2a-(2b-(2a-2b+x)) \\ &= 2a-(4b-2a-x)) \\ &= 4a-4b+x, \end{aligned}$$

so $[R_{a,\pi}, R_{b,\pi}] = T_{4(a-b)}$. On the other hand, we saw in lectures that $[R_{a,\theta}, R_{b,\phi}] = T_{(1-R_\theta)(1-R_\phi)(a-b)}$. This is consistent because $1-R_\pi$ is just twice the identity matrix, so $(1-R_\theta)(1-R_\phi)(a-b) = 4(a-b)$.

Exercise 2. Find $\text{Symm}(X)$ and $\text{Dir}(X)$ when $X \subseteq \mathbb{R}^2$ is

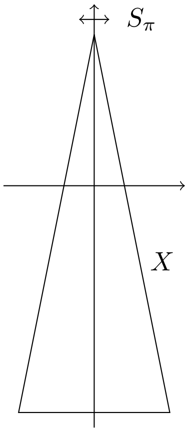
(a) The unit disc centred at the origin
(b) The isosceles triangle with vertices $(0,2)$, $(-1,-3)$ and $(1,-3)$.
(c) The four points $(1,1)$, $(1,-1)$, $(-1,1)$ and $(-1,-1)$.
(d) The square with vertices $(-1,2)$, $(-1,-2)$, $(3,2)$ and $(3,-2)$.

Solution:

(a) Here $\text{Symm}(X) = O_2$ and $\text{Dir}(X) = SO_2$. This just means that the unit disc is invariant under any rotation about the origin, and under any reflection across a line through the origin, which is geometrically clear.

For a more algebraic proof, note that $X = \{x \in \mathbb{R}^2 \mid \|x\| \leq 1\}$. For any $A \in O_2$ and $x \in X$ we have $\|Ax\| = \|x\| \leq 1$ so $Ax \in X$; thus $AX \subseteq X$. Conversely, if $y \in X$ then $\|A^{-1}y\| = \|y\| \leq 1$ so the point $x := A^{-1}y$ lies in X. We have $y = Ax$ so $y \in AX$. This shows that $X \subseteq AX$, so $X = AX$, so $A \in \text{Symm}(X)$. As A was an arbitrary element of O_2 we have $\text{Symm}(X) = O_2$ and $\text{Dir}(X) = \text{Symm}(X) \cap SO_2 = O_2 \cap SO_2 = SO_2$, as claimed.

(b) Here it is evident that the only symmetry is under reflection across the y-axis, which lies at angle $\pi/2$ to the horizontal. Recall that S_θ is the reflection across the line at angle $\theta/2$ to the horizontal, so reflection across the y-axis is S_π. Thus $\text{Symm}(X) = \{1, S_\pi\}$. This contains no rotations other than the identity, so $\text{Dir}(X) = \{1\}$.

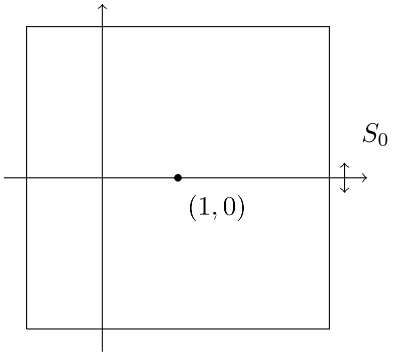


(c) Here X consists of the vertices of a square of side 2 with horizontal and vertical sides (note that this is different from our usual square X_4). We have $\text{Symm}(X) = D_4$ and $\text{Dir}(X) = C_4$. Indeed, it is clear that X is invariant under a rotation R_θ if and only if θ is a multiple of a quarter-turn, or in other words a multiple of $\pi/2 = 2\pi/4$. Thus if we put $R = R_{\pi/2}$ we find that

$$\text{Dir}(X) = \{1 = R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}\} = \{1, R, R^2, R^3\} = C_4.$$

It is also clear that X is unchanged if we reflect it across the x-axis, so $S_0 \in \text{Symm}(X)$. If $A \in \text{Symm}(X)$ is a reflection then AS_0 is a rotation and lies in $\text{Symm}(X)$ so $AS_0 = R^k$ for some k so $A = AS_0S_0 = R^kS_0$ so $A \in D_4$. If $A \in \text{Symm}(X)$ is a rotation we have seen that $A \in C_4 \subseteq D_4$, so again $A \in D_4$; thus $\text{Symm}(X) \subseteq D_4$. As R and S_0 preserve X we also have $D_4 \subseteq \text{Symm}(X)$, so $\text{Symm}(X) = D_4$. Alternatively, we can just observe geometrically that there are four lines of reflectional symmetry at angles 0, $\pi/4$, $\pi/2$ and $3\pi/4$ to the x-axis, so the reflections in $\text{Symm}(X)$ are S_0, $S_{\pi/2}$, S_π and $S_{3\pi/2}$.

(d) Here X is an off-centre square.



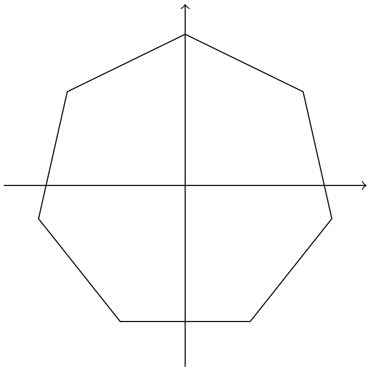
There is a lot of symmetry about the point $(1, 0)$ at the centre of the square. However, the question asks about $\text{Symm}(X)$, which is by definition the group of symmetries about the point $(0, 0)$, and from that point of view the picture is much less symmetrical. In fact, the only symmetry is the reflection across the x-axis, so $\text{Symm}(X) = \{1, S_0\}$ and $\text{Dir}(X) = \{1\}$.

Exercise 3. (a) What can you say about $R_\pi A R_\pi^{-1}$ for $A \in O_2$? (Try writing out the matrices explicitly).

(b) Show that $R_{\pi/n}X_n \neq X_n$ but that $D_n = R_{\pi/n}D_nR_{\pi/n}^{-1}$.

(c) Deduce that $R_{\pi k/n}D_nR_{\pi k/n}^{-1} = D_n$ for all $k \in \mathbb{Z}$.

(d) Let X be the regular heptagon centred at $(0, 0)$ with one vertex at $(0, 1)$. Find n and θ such that $\text{Symm}(X) = R_\theta D_n R_\theta^{-1}$. There are three different possibilities for θ in the range $[0, \pi/2)$; find all of them.



Solution:

(a) R_π is the matrix $\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)$, in other words $R_\pi = -I$. This means that $R_\pi^{-1} = -I$ also and thus that $R_\pi A R_\pi^{-1} = -(-A) = A$ for all A.

(b) The polygon X_n has vertices v_k with polar coordinates $[1, 2\pi k/n]$. The map $R_{\pi/n}$ sends v_0 to $[1, \pi/n]$ which is not a vertex, so $R_{\pi/n}X_n \neq X_n$. The elements of D_n have the form $R_{2k\pi/n}$ or $S_{2k\pi/n}$ for $k \in \mathbb{Z}$. Using the equations $R_\alpha R_\beta R_\alpha^{-1} = R_\beta$ and $R_\alpha S_\beta R_\alpha^{-1} = S_{\beta+2\alpha}$ we see that

$$R_{\pi/n}R_{2\pi k/n}R_{\pi/n}^{-1} = R_{2\pi k/n} \in D_n$$
$$R_{\pi/n}S_{2\pi k/n}R_{\pi/n}^{-1} = S_{2\pi(k+1)/n} \in D_n.$$

This shows that $R_{\pi/n}D_nR_{\pi/n}^{-1} \subseteq D_n$ but these two sets have the same size so they must actually be equal.

(c) If $R_{\pi k/n}D_nR_{\pi k/n}^{-1} = D_n$ then we can substitute $D_n = R_{\pi/n}D_nR_{\pi/n}^{-1}$ on the left hand side to deduce that

$$R_{\pi(k+1)/n}D_nR_{\pi(k+1)/n}^{-1} = R_{\pi k/n}R_{\pi/n}D_nR_{\pi/n}^{-1}R_{\pi k/n}^{-1} = R_{\pi k/n}D_nR_{\pi k/n}^{-1} = D_n.$$

By induction, this proves (c) for all $k \geq 0$. If $k < 0$ we have $k = -m$ for some $m > 0$ and we have proved already that $D_n = R_{\pi m/n}D_nR_{\pi m/n}^{-1}$. If we multiply this equation on the left by $R_{\pi m/n}^{-1}$ and on the right by $R_{\pi m/n}$ we obtain $R_{\pi - m/n}D_nR_{\pi m/n} = D_n$, or in other words $R_{\pi k/n}D_nR_{\pi k/n}^{-1} = D_n$, as required.

(d) We have $X = R_{\pi/2}X_7$ so

$$\mathrm{Symm}(X) = R_{\pi/2}\,\mathrm{Symm}(X_7)R_{\pi/2}^{-1} = R_{\pi/2}D_7R_{\pi/2}^{-1}.$$

More generally, by using part (c) we see that $R_{\pi k/7}D_7R_{\pi k/7}^{-1} = D_7$ and thus that

$$\mathrm{Symm}(X) = R_{\pi/2}D_7R_{\pi/2}^{-1} = R_{\pi/2}R_{\pi k/7}D_7R_{\pi k/7}^{-1}R_{\pi/2}^{-1} = R_{(2k+7)\pi/14}D_7R_{(2k+7)\pi/14}^{-1}.$$

Thus, if we put $\theta = (2k+7)\pi/14$ we again have $\mathrm{Symm}(X) = R_\theta D_7 R_\theta^{-1}$.

Conversely, suppose that θ satisfies $\mathrm{Symm}(X) = R_\theta D_7 R_\theta^{-1}$. We then have

$$D_7 = R_{\pi/2}^{-1}\,\mathrm{Symm}(X)R_{\pi/2} = R_{\pi/2}^{-1}R_\theta D_7 R_{\pi/2}R_\theta^{-1} = R_{\theta-\pi/2}D_7R_{\theta-\pi/2}^{-1}.$$

As $S_0 \in D_7$ this implies that the element $S_{2\theta-\pi} = R_{\theta-\pi/2}S_0R_{\theta-\pi/2}^{-1}$ also lies in D_7. However, we only have $S_\phi \in D_7$ if ϕ is a multiple of $2\pi/7$, so $2\theta - \pi = 2k\pi/7$ for some k, so $\theta = \pi/2 + k\pi/7 = (2k+7)\pi/14$. Thus we have $\mathrm{Symm}(X) = R_\theta D_7 R_\theta^{-1}$ if and only if θ has the form $(2k+7)\pi/14$ for some integer k. For $\theta \in [0, \pi/2)$ we must have $k = -3$ or $k = -2$ or $k = -1$, so $\theta \in \{\pi/14, 3\pi/14, 5\pi/14\}$.

Exercise 4. Prove that D_n is generated by reflections.

(A group G is said to be *generated* by a subset Y if every $g \in G$ can be written in the form

$$g = y_1^{a_1}y_2^{a_2}\cdots y_n^{a_n}$$

for some $n \geq 1$, $y_1, y_2, \ldots, y_n \in Y$ and $a_1, a_2, \ldots, a_n \in \{\pm 1\}$.)

Solution: Write $R = R_{2\pi/n}$ and $S = S_0$ so

$$D_n = \{1, R, \dots, R^{n-1}, S, RS, \dots, R^{n-1}S\}.$$

Using the fact that $R_\alpha S_\beta = S_{\alpha+\beta}$ we see that $R^kS = R_{2k\pi/n}S_0 = S_{2k\pi/n}$, which is a reflection. Also, because $S^2 = 1$ we see that $R^k = (R^kS)S$. Here R^kS and S are reflections lying in D_n, so R^k can be written as a product of two reflections lying in D_n. Thus every element in D_n is either a reflection or a product of reflections, so the reflections in D_n generate D_n as claimed.

Exercise 5. Find the conjugacy classes of the elements of D_n and hence find the centre of D_n. [Hint: First deal with the cases of D_1 and D_2 which are a bit different. Then treat D_3 and D_4. You are then probably ready for the general case. See also the case treated in lectures!]

Solution:

- $D_1 = \{1, S\}$; the conjugacy classes are $\{1\}$ and $\{S\}$.
- $D_2 = \{I, R, S, SR\}$. We have $R^2 = 1$ so $R = R^{-1}$. This means that $SRS = R^{-1} = R$, so $SR = RS$, so the group is commutative. This means that each element is in a separate conjugacy class, so the classes are $\{1\}$, $\{R\}$, $\{S\}$ and $\{SR\}$.
- $D_3 = \{1, R, R^2, S, SR, SR^2\}$. We have $R^3 = 1$ so $S^{-1}RS = R^{-1} = R^2$, showing that R and R^2 are conjugate.

Exercise 6. Use the First Isomorphism Theorem to prove that $SO_2 \simeq \mathbb{R}/2\pi\mathbb{Z}$.

Solution: Define $\phi\colon \mathbb{R} \to SO_2$ by $\phi(\alpha) = R_\alpha$. We have

$$\phi(\alpha)\phi(\beta) = R_\alpha R_\beta = R_{\alpha+\beta} = \phi(\alpha + \beta),$$

so ϕ is a homomorphism. Any element of SO_2 has the form $R_\alpha = \phi(\alpha)$ for some α, so ϕ is surjective. Thus, the First Isomorphism Theorem gives us an isomorphism $\overline{\phi}\colon \mathbb{R}/\ker(\phi) \to SO_2$. Moreover, we have $\alpha \in \ker(\phi)$ iff $\phi(\alpha) = 1$ iff $R_\alpha = R_0$ iff α is an integer multiple of 2π, so $\ker(\phi) = 2\pi\mathbb{Z}$. Thus $\mathbb{R}/2\pi\mathbb{Z} \simeq SO_2$ as claimed.

Exercise 7. Suppose $x_0, x_1, \dots x_n \in \mathbb{R}^n$ have the property that $x_1 - x_0, x_2 - x_0, \dots, x_n - x_0$ is a basis. If f, g are isometries of $\mathbb{R}^n$ so that $f(x_i) = g(x_i)$ for $i = 0, 1, 2, \dots, n$ then show that $f = g$. Thus for instance an isometry of $\mathbb{R}^2$ is determined by the image of three points.

Solution:

Exercise 8. Let $\mathbb{R}^\infty$ be the set of sequences $x = (x_1, x_2, \dots)$ such that $x_n = 0$ for $n \gg 0$. We define as usual

$$\begin{aligned} \langle x, y\rangle &= \sum_{k=1}^{\infty} x_k y_k \\ \|x\| &= \sqrt{\langle x, x\rangle} \\ d(x, y) &= \|x - y\|. \end{aligned}$$

Note that the infinite sum is really only a finite sum because when k is large we have $x_k = y_k = 0$. Thus, there is no convergence problem to worry about. Construct a function $f\colon \mathbb{R}^\infty \to \mathbb{R}^\infty$ that preserves distances but is not a bijection.

Solution: Define $f(x_1, x_2, x_3, \dots) = (0, x_1, x_2, x_3, \dots)$. This is a linear map, and it satisfies

$$\|f(x)\|^2 = 0^2 + x_1^2 + x_2^2 + \dots = \|x\|^2.$$

We thus have

$$d(f(x), f(y)) = \|f(x) - f(y)\| = \|f(x - y)\| = \|x - y\| = d(x, y),$$

so f preserves distances. However, the first entry in $f(x)$ is always 0, so $f(x)$ cannot be equal to $(1, 0, 0, \dots)$ for any x, so f is not surjective and thus not bijective.

Exercise 9. Find the conjugacy classes in O_2. What is the centre of O_2?

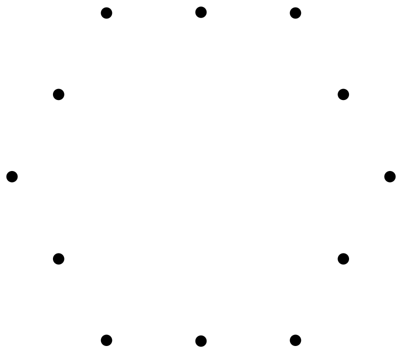
Solution:

Exercise 10. (a) Consider the action of O_2 on $\mathbb{R}^2$. Identify the orbits as subsets of $\mathbb{R}^2$ and draw a picture. Identify the stabilizers.

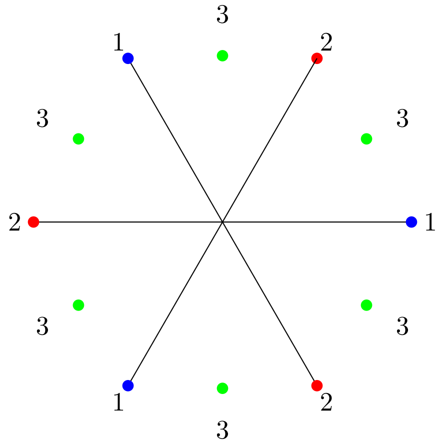
(b) Consider the action of $I(\mathbb{R}^2)$ on $\mathbb{R}^2$. Identify the orbits as subsets of $\mathbb{R}^2$ and draw a picture. Identify the stabilizers.

Solution:

Exercise 11. Let X be the following subset of $\mathbb{R}^2$ (with centre at the origin). The group D_3 acts on X. Find the orbits of this action, find the fixed points of all the elements of D_3, and verify the orbit counting theorem.



Solution: The points marked 1 form an orbit of size 3, the points marked 2 form another orbit of size 3, and the points marked 3 form an orbit of size 6. Thus, there are 3 orbits altogether.



Recall that

$$D_3 = \{1, R_{2\pi/3}, R_{4\pi/3}, S_0, S_{2\pi/3}, S_{4\pi/3}\}.$$

The identity element of D_3 fixes all 12 points of X. The rotations $R_{2\pi/3}$ and $R_{4\pi/3}$ have no fixed points in X. The axis of the reflection S_0 passes through 2 of the points of X. These two points are fixed under S_0, and the remaining points are not. Similarly, the reflections $S_{2\pi/3}$ and $S_{4\pi/3}$ have two fixed points each. Thus

$$\frac{1}{|G|}\sum_{g\in G} |\operatorname{Fix}(g)| = \frac{1}{6}(12+0+0+2+2+2) = 3,$$

which is equal to the number of orbits, as predicted by the orbit counting theorem.

Exercise 12. Find an infinite subgroup $G < SO_2$ such that $G \neq SO_2$. [Hint: think about rational and irrational numbers.]

Solution: One possibility is to choose an irrational number α and define $R = R_{2\pi\alpha}$ and

$$G = \langle R\rangle = \{R^n \mid n \in \mathbb{Z}\} = \{R_{2\pi\alpha n} \mid n \in \mathbb{Z}\}.$$

This is clearly a subgroup of SO_2 (because $1 = R^0 \in G$ and $R^n R^m = R^{n+m} \in G$ and $(R^n)^{-1} = R^{-n} \in G$ for all $n, m \in \mathbb{Z}$.)

I next claim that all the elements R^n are distinct, in other words that $R^n \neq R^m$ whenever $n \neq m$. Indeed, if $R^n = R^m$ then $R_{2\pi\alpha(n-m)} = R^{n-m} = 1$ so $2\pi\alpha(n-m) = 2\pi k$ for some integer k. If $n \neq m$ then this implies that $\alpha = k/(n-m)$, contradicting our assumption that α is irrational. This proves that the elements R^n are all distinct, so G is infinite.

Finally we must prove that $G \neq SO_2$. For those of you that know about countability, the "real reason" is that G is countable and SO_2 is not. For a more direct proof, it will suffice to show that $R_\pi \notin G$. If R_π were an element of G we would have $R_\pi = R^k$ for some $k \in \mathbb{Z}$, and $k \neq 0$ because certainly $R_\pi \neq 1 = R^0$. This would give $R^{2k} = R_\pi^2 = 1 = R^0$, contradicting the fact that all the R^n's are distinct.

Two other possibilities are to take $G = \{R_{a\pi} \mid a \in \mathbb{Q}\}$ or to take $G = \{R_\theta \mid \theta \in \mathbb{Q}\}$.

Exercise 13. Put $H_n = \{A \in O_2 \mid A^n = 1\}$. Show that if n is odd then H_n is a finite subgroup of O_2 (which one?), but if n is even then H_n is not a subgroup at all.

Solution: First suppose that n is odd, say $n = 2m+1$. For any θ we have $S_\theta^2 = 1$ so $S_\theta^n = (S_\theta^2)^m S_\theta = S_\theta \neq 1$, so $S_\theta \notin H_n$. On the other hand, we have $R_\theta^n = 1$ iff $n\theta = 2k\pi$ for some $k \in \mathbb{Z}$, iff $\theta = 2k\pi/n$ for some k, iff $R_\theta \in C_n$. Thus $H_n = C_n$, which is a finite subgroup of O_2.

Now suppose instead that n is even, say $n = 2m$. Then for all θ we have $S_\theta^n = (S_\theta^2)^m = 1$, so $S_\theta \in H_n$. For most θ we have $R_\theta^n \neq 1$, so $R_\theta \notin H_n$. Thus S_θ and S_0 lie in H_n but $S_\theta S_0 = R_\theta$ does not; this shows that H_n is not a subgroup.

Exercise 14. Show that if $G/Z(G)$ is a cyclic group then G is abelian (hence in fact $Z(G) = G$). Identify $D_4/Z(D_4)$.

Solution:

Exercise 15. The Quaternion group of order 8 is the group

$$G = \{\pm 1, \pm i, \pm j, \pm k\}$$

with $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, $i^2 = j^2 = k^2 = -1$. Do there exist subgroups $N, Q < G$ (with $N \neq G$ and $Q \neq G$) such that G is the semidirect product of N and Q? (One approach is just to find all the subgroups of G).

Solution: No such subgroups exist. To prove this, I first claim that any nontrivial subgroup $H \leq G$ contains the element -1. Indeed, we have $G = \{1, -1, i, -i, j, -j, k, -k\}$ and $i^2 = (-i)^2 = j^2 = (-j)^2 = k^2 = (-k)^2 = -1$. As H is nontrivial it must either contain -1 (so there is nothing to say) or some element $h \in \{\pm i, \pm j, \pm k\}$, in which case it also contains $h^2 = -1$, as claimed.

Now suppose that G is the semidirect product of N and Q, where $N \neq G$ and $Q \neq G$. We then have $|N| < |G|$ so $|Q| = |G|/|N| > 1$, so Q is nontrivial, so $-1 \in Q$. Similarly $-1 \in N$, so $-1 \in N \cap Q$. However, for a semidirect product we must have $N \cap Q = \{1\}$, so this gives a contradiction.

The complete list of subgroups is as follows:

$$\begin{aligned}
&\{1\}\\
&\{1, -1\}\\
&\{1, -1, i, -i\}\\
&\{1, -1, j, -j\}\\
&\{1, -1, k, -k\}\\
&\{1, -1, i, -i, j, -j, k, -k\}.
\end{aligned}$$

Exercise 16. If X is a non-empty subset of a group G, we write

$$\langle X \rangle = \{x_1^{\varepsilon_1} \cdots x_t^{\varepsilon_t} \mid t \geq 1,\ x_1, \cdots, x_t \in X,\ \varepsilon_1, \cdots \varepsilon_t \in \{\pm 1\}\}$$

and call it the subgroup of G generated by X.

Suppose G is a group with elements $a, b \in G$, so that $G = \langle a, b \rangle$. Show that if a and b are of order 2 and ab is of order n then $G \cong D_n$.

Solution:

Exercise 17. Use your classification of the conjugacy classes in D_n to find all the normal subgroups of D_n.

Solution:

Exercise 18. Let G be a subgroup of SO_2. Suppose that there exists a number $\epsilon > 0$ such that $R_\theta \notin G$ for $0 < \theta < \epsilon$. Prove that $G = C_n$ for some n (and thus that G is finite). [Hint: mimic the classification of finite subgroups of C_n.]

Solution: Put $S = \{\phi > 0 \mid R_\phi \in G\}$, so $2\pi \in S$. If we take $m = 1$ then by assumption we have $S \cap (0, m\epsilon) = \emptyset$. If we take m to be very large then $2\pi \in S \cap (0, m\epsilon)$ so $S \cap (0, m\epsilon) \neq \emptyset$. Thus, there must be some intermediate value of m such that $S \cap (0, m\epsilon) = \emptyset$ and $S \cap (0, (m+1)\epsilon) \neq \emptyset$. Choose $\theta \in S \cap (0, (m+1)\epsilon)$. I claim that for $\phi \in S$ we have $\phi \geq \theta$. Suppose not, so $\phi < \theta$. Put $\psi = \theta - \phi$, so $\psi > 0$ and $R_\psi = R_\theta R_\phi^{-1} \in G$ so $\psi \in S$. We also have $\theta < (m+1)\epsilon$. As $S \cap (0, m\epsilon) = \emptyset$ we certainly have $\phi \geq m\epsilon$, so $\psi = \theta - \phi < (m+1)\epsilon - m\epsilon = \epsilon$. This contradicts the assumption that $S \cap (0, \epsilon) = \emptyset$, so we must have $\phi \geq \theta$ after all.

Now let α be any element of S. For some $k \geq 0$ we must have $k\theta \leq \alpha < (k+1)\theta$. If we put $\beta = \alpha - k\theta$ then $0 \leq \beta < \theta$ and $R_\beta = R_\alpha R_\theta^{-k} \in G$. As every element of S is at least as large as θ we see that β cannot lie in S, and the only way this can happen is if $\beta = 0$. Thus $\alpha = k\theta$ for some $k > 0$.

By applying this in the case $\alpha = 2\pi$ we see that $2\pi = n\theta$ for some n and thus that $\theta = 2\pi/n$. It follows that $S = \{2\pi k/n \mid k > 0\}$ and thus that $G = C_n$.

Exercise 19. The quaternion group of order 8 is the group

$$G = \{\pm 1, \pm i, \pm j, \pm k\}$$

with $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, $i^2 = j^2 = k^2 = -1$. Show that if P and Q are any two nontrivial subgroups of G, then $P \cap Q$ is also nontrivial.

Solution: We first claim that any nontrivial subgroup $P \leq G$ contains the element -1. Indeed, we have $G = \{1, -1, i, -i, j, -j, k, -k\}$ and $i^2 = (-i)^2 = j^2 = (-j)^2 = k^2 = (-k)^2 = -1$. As P is nontrivial it must either contain -1 (so there is nothing to say) or some element $x \in \{\pm i, \pm j, \pm k\}$, in which case it also contains $x^2 = -1$, as claimed. By the same argument, Q must contain -1, so $P \cap Q$ contains -1, so $P \cap Q$ is nontrivial.

Exercise 20. Prove or disprove the following statements:

(i) $D_6/Z(D_6) \simeq D_3$, where $Z(D_6)$ is the centre of D_6.
(ii) D_{42} has a non-cyclic subgroup of order 21.
(iii) $D_8 \simeq D_4 \times C_2$.
(iv) There is an integer $n \geq 1$ such that there is a surjective homomorphism $D_n \to Q_8$.
(v) $D_{10} \cong D_5 \times C_2$.

Solution:

Exercise 21. Let $\delta\colon I_n \to \{\pm 1\}$ be the composite of $\psi\colon I_n \to I_n/T_n \simeq O_n$ and the determinant map (ie $\delta(f) = \det(\psi(f))$).

(a) If $f \in O_n$ show that $\delta(f) = \det(f)$.
(b) When $n = 2$ find the value of δ on reflections, rotations, translations and glides.
(c) If $X \subseteq \mathbb{R}^n$ write

$$SI(X) = \{f \in I(X) \mid \delta(f) = 1\}.$$

Show that $SI(X)$ is a subgroup of $I(X)$ and that either $SI(X) = I(X)$ or $[I(X) : SI(X)] = 2$.

Solution:

Exercise 22. Let $f, g \in I_n$ be given by $f(x) = Ax + a$ and $g(x) = Bx + b$, where $A, B \in O_n$ and $a, b \in \mathbb{R}^n$.

(a) Find $C \in O_n$ and $c \in \mathbb{R}^n$ such that $fg(x) = Cx + c$ for all x.
(b) Find D and d such that $fgf^{-1}(x) = Dx + d$ for all x.
(c) Describe the isometry fT_bf^{-1}.

(d) Show that $T_{(1,0)}$ is not conjugate to $T_{(0,2)}$ in I_2.

Solution:

(a) We have $fg(x) = f(Bx+b) = A(Bx+b)+a = ABx + (Ab+a)$, so we can take $C = AB$ and $c = Ab + a$.

(b) First, if $x = f(y) = Ay + a$ then $f^{-1}(x) = y = A^{-1}(x-a) = A^{-1}x - A^{-1}a$. Thus

$$\begin{aligned} fgf^{-1}(x) &= fg(A^{-1}x - A^{-1}a) \\ &= f(BA^{-1}x - BA^{-1}a + b) \\ &= ABA^{-1}x - ABA^{-1}a + Ab + a. \end{aligned}$$

Thus we can take $D = ABA^{-1}$ and $d = a + Ab - ABA^{-1}a$.

(c) This is what we get in the case $B = 1$. We then have $ABA^{-1} = 1$, so part (b) gives $fT_bf^{-1}(x) = x - a + Ab + a = x + Ab = T_{Ab}(x)$, so $fT_bf^{-1} = T_{Ab}$.

(d) If T_b is conjugate to T_c then $T_c = fT_bf^{-1}$ for some $f \in I_2$. If we write f in the form $f(x) = Ax + a$ (with $A \in O_2$), we see from (c) that $fT_bf^{-1} = T_{Ab}$, so $Ab = c$. Thus $\|c\| = \|Ab\| = \|b\|$. As $\|(1,0)\| \neq \|(0,2)\|$, we deduce that $T_{(1,0)}$ is not conjugate to $T_{(0,2)}$.

Exercise 23. Let H be a wallpaper group, and let a be a point in $\mathbb{R}^2$. Recall that $\text{orbit}_H(a) = \{h(a) \mid h \in H\}$. Prove that if $\text{orbit}_H(a) = \text{orbit}_{T(H)}(a)$ then $\sigma_a(H) = \psi(H)$.

Solution: For any group $H \leq I_2$ we have seen that $\sigma_a(H) \leq \psi(H)$, so we need only prove the opposite inequality. Suppose that $B \in \psi(H)$, so there is some element $h \in H$ with $\psi(h) = B$. We have $h(a) \in \text{orbit}_H(a) = \text{orbit}_{T(H)}(a)$, so there must be some $u \in T(H)$ such that $h(a) = a + u$. Put $g = T_{-u}h$, so $g \in H$ and $g(a) = a$. This means that the map $f := T_{-a}gT_a$ satisfies $f(0,0) = (0,0)$, so $f(x) = Ax$ for some $A \in O_2$. From the definition of $\sigma_a(H)$ we see that $A \in \sigma_a(H)$. On the other hand, we have

$$A = \psi(f) = \psi(T_{-a}gT_a) = \psi(T_{-u-a}hT_a) = \psi(T_{-u-a})\psi(h)\psi(T_a) = 1.B.1 = B,$$

so $A = B$. As $A \in \sigma_a(H)$, this means that $B \in \sigma_a(H)$, as required.

Exercise 24. Let H be a wallpaper group, and put $L = \{h(0) \mid h \in H\}$. Prove that $H \cap O_2 \leq \psi(H)$. Prove also that if $L = \text{Trans}(H)$, then $\psi(H) = H \cap O_2$.

Solution: First, if $A \in O_2$ then $A = \psi(A)$. Thus, if $A \in H \cap O_2$ then $A = \psi(A) \in \psi(H)$, so $H \cap O_2 \leq \psi(H)$.

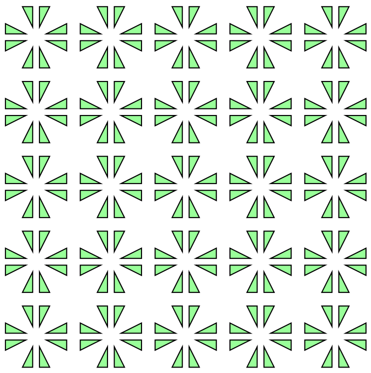
Now suppose that $L = \text{Trans}(H)$; we must show that $\psi(H) \leq H \cap O_2$. If $A \in \psi(H)$ then there is an element $h \in H$ with $\psi(h) = A$, which means that $h(x) = Ax + a$ for some $a \in \mathbb{R}^2$. Next, note that $a = h(0)$, so $a \in L$ (by the definition of L). We are assuming that $L = \text{Trans}(H)$, so $a \in \text{Trans}(H)$, which means that $T_a \in H$. This means that the function $g = T_a^{-1}h$ also lies in H. Clearly $g(x) = h(x) - a = Ax$, so g corresponds to the element $A \in O_2$. This means that $A \in H \cap O_2$, as claimed.

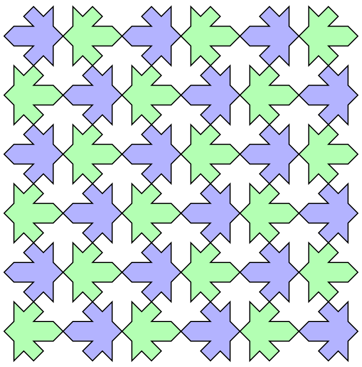
Exercise 25. Three infinite wall-paper patterns are represented below by a small segment of the pattern.

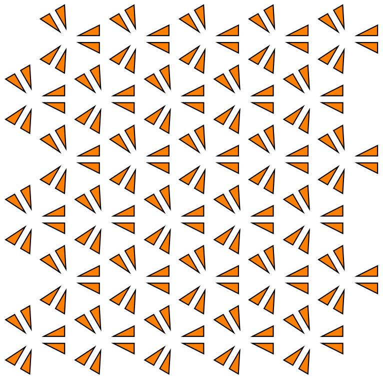
(a) Find the isometry group of pattern (a).

(b) Find the isometry group of pattern (b).

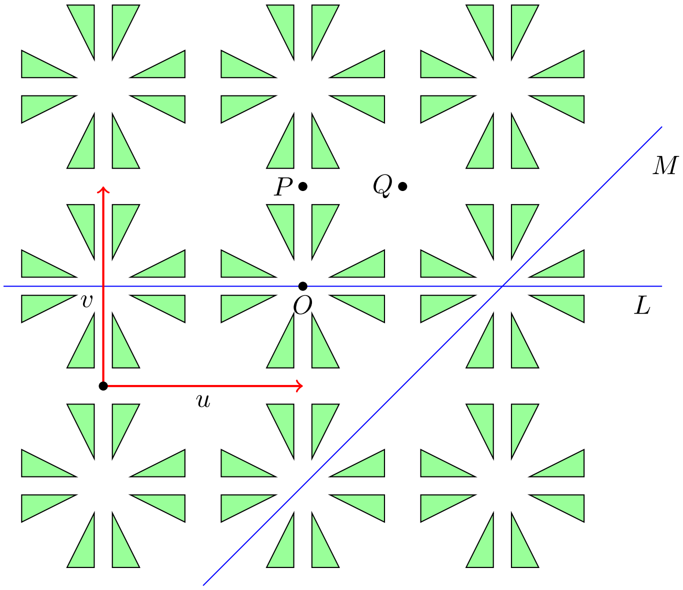
(c) Find the isometry group of pattern (c) and show that it is generated by a reflection and a rotation.


Pattern (a)


Pattern (b)

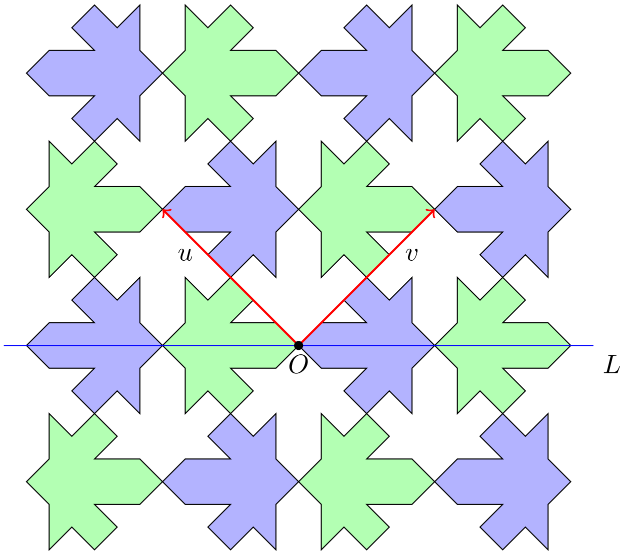

Pattern (c)

Solution: Pattern (a): Let R be rotation throught $\pi/2$ about O, and let S be reflection across L. It is clear that T_u, T_v, R and S preserve X, so $\langle T_u, T_v, R, S\rangle \leq I(X)$. Now suppose we have $f_0 \in I(X)$. If $\det(f_0) = -1$ we put $f_1 = Sf_0$, otherwise we put $f_1 = f_0$; either way we have $\det(f_1) = 1$ and $f_1 \in I(X)$. Clearly f_1 must send O to the centre of one of the motifs, so $f_1(O) = nu+mv+O$ for some $n, m \in \mathbb{Z}$. We put $f_2 = T_u^{-n}T_v^{-m}f_1$, so $f_2 \in I(X)$, $\det(f_2) = 1$ and $f_2(O) = O$. Thus f_2 is a rotation about O that preserves X; clearly the angle must be a multiple of $\pi/2$, so $f_2 = R^k$ for some k. We thus have $f_1 = T_v^m T_u^n R^k$ and either $f_0 = T_v^m T_u^n R^k$ or $f_0 = ST_v^m T_u^n R^k$. Thus $f_0 \in \langle T_u, T_v, R, S\rangle$, which proves that $I(X) = \langle T_u, T_v, R, S\rangle$.

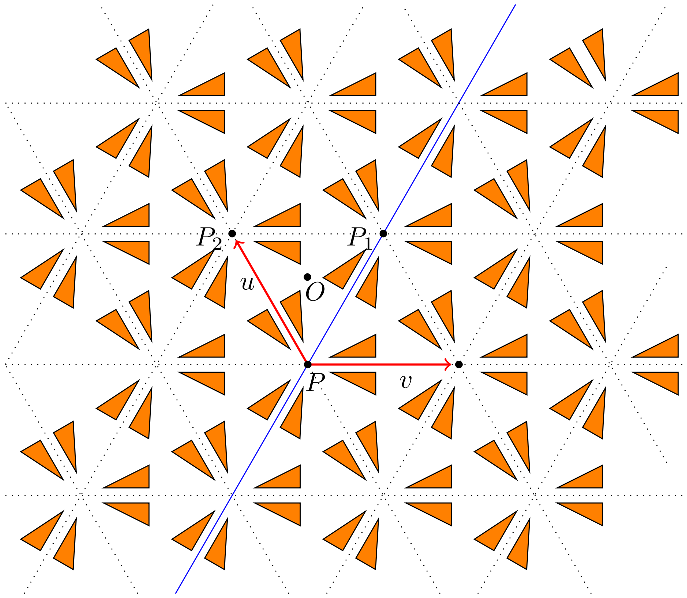


In particular, we see that S_M, $R_{P,\pi}$ and $R_{Q,\pi/2}$ all lie in $\langle T_u, T_v, R, S\rangle$. By following the above recipe we find that $S_M = ST_vT_uR$, $R_{P,\pi} = T_vR^2$ and $R_{Q,\pi/2} = T_uR$.

Pattern (b): Clearly $\langle T_u, T_v, S_L\rangle \leq I(X)$. Suppose that $f_0 \in I(X)$, and put $f_1 = S_Lf_0$ if $\det(f_0) = -1$ and $f_1 = f_0$ otherwise. Note that O is the point where the blunt ends of two white motifs meet, so $f_1(O)$ must also be the point of intersection of the blunt ends of two white motifs, so $f_1(O) = O + nu + mv$ for some $n, m \in \mathbb{Z}$. Put $f_2 = T_u^{-n}T_v^{-m}f_1$, so f_2 is a rotation around O that preserves the pattern X. There is only one dark grey motif adjacent to O, so f_2 must send that motif to itself, and this forces f_2 to be the identity. Thus either $f_0 = T_v^m T_u^n$ or $f_0 = S_L T_v^m T_u^n$, and in either case we have $f_0 \in \langle S_L, T_u, T_v\rangle$. This shows that $I(X) = \langle S_L, T_u, T_v\rangle$.

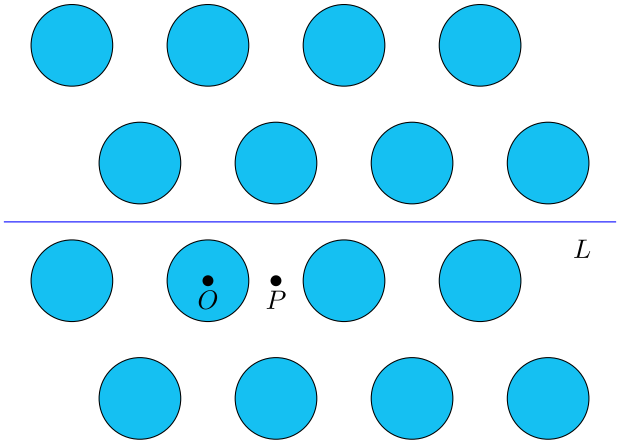


Pattern (c): Put $S = S_L$ and $R = R_{O,2\pi/3}$, so $\langle R, S\rangle \leq I(X)$.



As $\psi(S)$ is a reflection and $\psi(R)$ is a rotation we see that $\psi(RS) = \psi(R)\psi(S)$ is a reflection and thus that $\psi(RSRS) = \psi(RS)^2 = 1$, so $RSRS$ is a translation. As P lies on L we have $S(P) = P$ and $RS(P) = R(P) = P_1$. This lies on L again, so $SRS(P) = S(P_1) = P_1$, and it follows that $RSRS(P) = R(P_1) = P_2$. Thus $RSRS$ is a translation sending O to P_2, so we must have $RSRS = T_u$. Similarly, we have $SRSR = T_v$. Next, put $R' = T_u^{-1}T_v^{-1}R$. This has $\psi(R') = R_{2\pi/3}$, so R' must be a rotation through $2\pi/3$ about some point. We have seen that $R(P) = P_1 = P + u + v$ so $R'(P) = P$ so P must be the centre of the rotation R', so $R' = R_{P,2\pi/3}$. Now suppose that $f \in I(X)$. Then f must send P to the centre of some motif, say $f(P) = nu + mv$ for some $n, m \in \mathbb{Z}$, so $T_v^{-m}T_u^{-n}f$ fixes P and preserves X. After multiplying by S if necessary we get a rotation that fixes P and preserves X, which must be a power of R'. As T_u, T_v, S and R' lie in $\langle R, S\rangle$ we deduce that $f \in \langle R, S\rangle$. Thus $I(X) = \langle R, S\rangle$ as required.

Exercise 26. Let X be the wallpaper pattern shown below. We have seen that $I(X) = \langle T_u, T_v, R_{\pi/3}, S_0\rangle$, where $u = (1, 0)$ and $v = (1/2, \sqrt{3}/2)$. We also see geometrically that the rotation $R_{P,\pi}$ and the glide $G_{L,u/2}$ preserve X, so it must be possible to write $R_{P,\pi}$ and $G_{L,u/2}$ in terms of T_u, T_v, $R_{\pi/3}$ and S_0. Do this explicitly. [Hint: just follow through the steps in the proof that $I(X) = \langle T_u, T_v, R_{\pi/3}, S_0\rangle$.]



Solution: We have

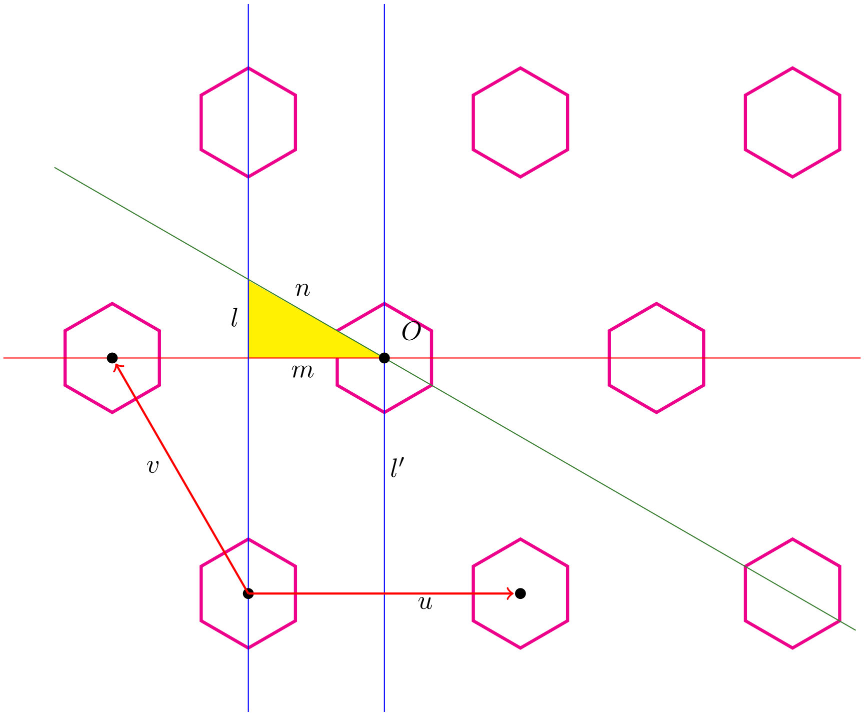
$$G_{L,u/2}(0,0) = u/2 + S_L(0,0) = (1/2,0) + (0,\sqrt{3}/2) = v,$$

so the map $f = T_{-v}G_{L,u/2} = T_{u/2-v}S_L$ satisfies $f(0,0) = (0,0)$. As L is parallel to the x-axis we have $\psi(S_L) = S_0$ and $\psi(T_a) = 1$ for all a so $\psi(f) = S_0$. Thus $f(x) = S_0(x) + b$ for some b, but $f(0,0) = (0,0)$ so $b = (0,0)$ so $f = S_0$. Thus $G_{L,u/2} = T_v f = T_v S_0$, which writes $G_{L,u/2}$ in terms of $\{T_u, T_v, R_{\pi/3}, S_0\}$ as required.

Similarly, we have $R_{P,\pi}(0,0) = (1,0) = u$ so the map $h = T_{-u}R_{P,\pi}$ satisfies $h(0,0) = (0,0)$. It also has $\psi(h) = \psi(T_{-u})\psi(R_{P,\pi}) = R_\pi$ so we must have $h = R_\pi$, so $R_{P,\pi} = T_u R_\pi = T_u R_{\pi/3}^3$.

Exercise 27. Let T be a triangle with angles $\pi/2$, $\pi/6$ and $\pi/3$. Let S_l, S_m and S_n be the reflections in the three sides of T. Find a pattern X with isometry group $\mathrm{Isom}(X)$ generated by S_l, S_m and S_n.

Solution: Let X be the pattern of hexagons shown below.



I claim that $I(X) = \langle S_l, S_m, S_n\rangle$. One checks directly that S_l, S_m and S_n send X to itself, so $\langle S_l, S_m, S_n\rangle \leq I(X)$. Clearly $S_m = S_0$ and $S_n = S_{-2\pi/6}$ and it follows that $\langle S_m, S_n\rangle = D_6$. Moreover, the $S_{l'} = S_\pi$ lies in D_6 so it can be written in terms of S_n and S_m (an explicit expression is $S_{l'} = S_n S_m S_n S_m S_n$). It follows that the map $T_u = S_{l'} S_l$ lies in $\langle S_l, S_m, S_n\rangle$. We also have $S_m S_n = R_{\pi/3}$ so the map $T_v = T_{R_{\pi/3}u} = R_{\pi/3} T_u R_{\pi/3}^{-1}$ also lies in $\langle T_l, T_m, T_n\rangle$. Given an arbitary element $g \in I(X)$ we see in the usual way that the map $h = T_u^{-n}T_v^{-m}g$ fixes O for some $n, m \in \mathbb{Z}$, and thus h lies in the symmetry group of the hexagon around O, which is the group $D_6 = \langle S_m, S_n\rangle$. It follows that the map $g = T_v^m T_u^n h$ lies in $\langle S_l, S_m, S_n\rangle$, which proves that $I(X) = \langle S_l, S_m, S_n\rangle$ as claimed.

Exercise 28. (a) Let the group G act on the non empty set X. We say that G acts *transitively* on X if for all $x, y \in X$ there is an element $g \in G$ so that $g * x = y$.

Show that the following are equivalent

(1) G acts transitively on X
(2) For any $z \in X$ we have $G * z = X$
(3) For some $z \in X$ we have $G * z = X$.

(b) Decide which of the following actions are transitive.

(1) S_n acting naturally on $\{1, 2, \ldots, n\}$.
(2) D_4 acting on the square X_4.
(3) S_6 acting by conjugation on the set of elements of S_6 having order 3 (so $\theta * \phi = \theta\phi\theta^{-1}$).

(c) Let G be a group and H be a subgroup. Then G acts on $G/H = \{xH \mid x \in G\}$, the set of left cosets of H in G, by left multiplication: $g * xH = gxH$, for $g \in G$ and $xH \in G/H$. Show G acts transitively on G/H.

(d) If G acts on sets X_1 and X_2 by $\bullet\colon G \times X_1 \to X_1$ and $*\colon G \times X_2 \to X_2$ we say these actions are *equivalent* if there is a bijection $\phi\colon X_1 \to X_2$ such that $g * \phi(x) = \phi(g \bullet x)$ for all $g \in G$ and $x \in X_1$.

Show that if G acts transitively on a set X then this action is equivalent to one of G by left multiplication on G/H, for some subgroup H of G.

Solution:

(a) (1)⇒(2): Suppose G acts transitively and that $z \in X$. Then for any $y \in X$ there exists $g \in G$ such that $g * z = y$, by the definition of transitivity. This means that $y \in \{g * z \mid g \in G\} = G * z$. As every y lies in $G * z$, we have $G * z = X$, as required.

(2)⇒(3): if the condition $G * z = X$ holds for every element z of the nonempty set X, then it certainly holds for some element.

(3)⇒(1): Suppose that $G * z = X$ for some element $z \in X$. Let x and y be points of X. Then $x \in X = G * z$, so $x = a * z$ for some $a \in G$. Similarly $y = b * z$ for some $b \in G$. Thus the element $g = ba^{-1}$ satisfies $g * x = (ba^{-1}) * a * z = b * z = y$. Thus G acts transitively, as claimed.

(b) (1) Suppose $x, y \in \{1, \ldots, n\}$. If $x = y$ let $\sigma \in S_n$ be the identity permutation, otherwise let σ be the transposition $(x\ y)$. Either way we have $\sigma * x = y$, so the action is transitive.

(2) This action is not transitive. The square X_4 contains the point $P = (1, 0)$, and also the point $Q = (1/2, 1/2)$ on the edge between $(1, 0)$ and $(0, 1)$. There is no element $g \in D_4$ such that $g(P) = Q$.

(3) This action is not transitive. To see this, put $x = (1\ 2\ 3)$ and $y = (1\ 2\ 3)(4\ 5\ 6)$. It is easy to see that $x^3 = y^3 = 1$, so x and y lie in the set under consideration. As x and y have different cycle types, they are not conjugate. More explicitly, for any $g \in S_6$ the permutation $g * x = gxg^{-1}$ satisfies $(gxg^{-1})(g(4)) = g(4)$, but there is no number i with $y(i) = i$, so $g * x \neq y$.

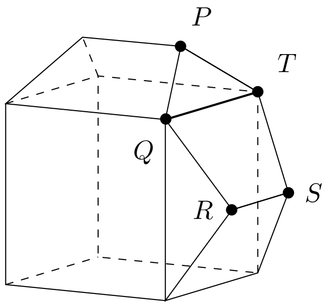
(c) Given any two elements $xH, yH \in G/H$, the element $g = yx^{-1}$ satisfies $g * (xH) = yH$; this shows that G acts transitively.

(d) Suppose that G acts transitively on X. Choose a point $a \in X$ and put $H = \{g \in G \mid g * a = a\}$. Define $\phi\colon G/H \to X$ by $\phi(xH) = x * a$. To see that this is well-defined, note that if $xH = yH$ then $x^{-1}y \in H$ so $(x^{-1}y) * a = a$ so $x * a = x * (x^{-1}y) * a = y * a$. Conversely, if $\phi(xH) = \phi(yH)$ then $x * a = y * a$ so $a = (x^{-1}y) * a$ so $x^{-1}y \in H$ so $xH = yH$; this shows that ϕ is injective. Moreover, for any $b \in X$, there is an element $x \in G$ with $x * a = b$, because the action is transitive, and so $\phi(xH) = b$. This shows that ϕ is surjective and thus bijective. We also have

$$\phi(g * (xH)) = \phi(gxH) = (gx) * a = g * (x * a) = g * \phi(xH),$$

so ϕ gives an equivalence between the two actions.

Exercise 29. Using the formulae in the notes about the geometry of the tent, find the coordinates of the vertices P, Q, R, S and T of the dodecahedron, as indicated in the diagram below.



Then find the centre C of the pentagon $PQRST$ and check that $d(P,C)^2 = d(Q,C)^2 = d(R,C)^2 = (2+\tau)/5$.

[**Hint:** You may find it convenient to write all numbers in terms of τ. If a $\sqrt{5}$ turns up you can write it as $2\tau - 1$ (because $\tau = (\sqrt{5}+1)/2$). If a τ^2 turns up you can write it as $\tau + 1$ (because $\tau^2 - \tau - 1 = 0$).]

Solution: The cube in the middle has centre at $(0,0,0)$ and the sides have length τ so the coordinates of the vertices are $(\pm\tau/2, \pm\tau/2, \pm\tau/2)$. We use the usual axes so the z-axis is vertical, the x-axis passes through the middle of RS and the y-axis is parallel to RS. With these conventions we have $Q = \tau/2.(1,-1,1)$ and $T = \tau/2.(1,1,1)$. Next, the right hand face of the cube has $x = \tau/2$ and we see from the notes that the distance from the base of a tent to its ridge is $1/2$ so on the line RS we have $x = \tau/2 + 1/2 = (\tau+1)/2$. The midpoint of RS lies on the x-axis and thus has coordinates $((\tau+1)/2, 0, 0)$. To get from this point to S we move half the length of the ridge in the positive y-direction. The length of the ridge is 1 so we end up with $S = ((\tau+1)/2, 0, 0) + (0, 1/2, 0) = (\tau+1, 1, 0)/2$. Similarly we have $R = (\tau+1, -1, 0)/2$.

Again, the top face is at height $\tau/2$ so the top ridge is at height $\tau/2 + 1/2 = (\tau+1)/2$ so the centre of the top ridge is $(0, 0, \tau+1)/2$. To get to P we move a distance of $1/2$ in the positive x-direction, so $P = (1, 0, \tau+1)/2$.

We now find that $Q + T = (\tau, 0, \tau)$ and $R + S = (\tau+1, 0, 0)$ so $P + Q + R + S + T = (2\tau + 3/2, 0, \tau + 1/2)$, so

$$C = (P+Q+R+S+T)/5 = (3+4\tau, 0, 1+3\tau)/10.$$

This implies that

$$\begin{aligned}
P - C &= (2-4\tau, 0, 4+2\tau)/10 \\
Q - C &= (-3+\tau, -5\tau, -1+2\tau)/10 \\
R - C &= (2+\tau, -5, -1-3\tau)/10.
\end{aligned}$$

It follows that

$$\begin{aligned}
d(P,C)^2 = \|P-C\|^2 &= ((2-4\tau)^2 + 0^2 + (4+2\tau)^2)/10^2 \\
&= (4 - 16\tau + 16\tau^2 + 16 + 16\tau + 4\tau^2)/100 \\
&= (1+\tau^2)/5 \\
&= (\tau+2)/5,
\end{aligned}$$

where we have used the relation $\tau^2 = \tau + 1$. Similarly, we have

$$\begin{aligned}
d(Q,C)^2 &= ((-3+\tau)^2 + 25\tau^2 + (-1+2\tau)^2)/100 \\
&= (9 - 6\tau + \tau^2 + 25\tau^2 + 1 - 4\tau + 4\tau^2)/100 \\
&= (1 - \tau + 3\tau^2)/10 \\
&= (2\tau+4)/10 = (\tau+2)/5,
\end{aligned}$$

and

$$\begin{aligned}
d(R,C)^2 &= ((2+\tau)^2 + 25 + (1+3\tau)^2)/100 \\
&= (4 + 4\tau + \tau^2 + 25 + 1 + 6\tau + 9\tau^2)/100 \\
&= (3 + \tau + \tau^2)/10 \\
&= (4+2\tau)/10 = (2+\tau)/5.
\end{aligned}$$

Exercise 30. This problem is a more elaborate application of the method we used to prove that the number $\tau = 2\cos(\pi/5)$ is equal to $(1+\sqrt{5})/2$.

Define $\zeta = e^{2\pi i/15}$ and $\sigma = \zeta + \zeta^{-1}$. Express the number $\rho = \sigma^4 - \sigma^3 - 4\sigma^2 + 4\sigma + 1$ in terms of ζ. Then work out $(\sigma+1)\rho$ and $(\zeta^5-1)\zeta^5(\sigma+1)\rho$. Show that $\zeta^5 \neq 1$ and that σ is a positive real number, and deduce that $\rho = 0$.

Now recall that the number $\tau = (1+\sqrt{5})/2$ satisfies $\tau^2 - \tau - 1 = 0$ so $\tau^{-1} = \tau - 1$ and $\tau - \tau^{-1} = 1$. Check that for any t we have $t^4 - t^3 - 4t^2 + 4t + 1 = q_0(t)q_1(t)$, where

$$\begin{aligned} q_0(t) &= t^2 - \tau t + \tau^{-1} - 1 \\ q_1(t) &= t^2 + \tau^{-1}t - \tau - 1. \end{aligned}$$

Deduce that either $q_0(\sigma) = 0$ or $q_1(\sigma) = 0$. Given that in fact $q_1(\sigma) \neq 0$, prove that $\sigma = (\tau + \sqrt{9-3\tau})/2$.

Solution: First, we have

$$\begin{aligned} \sigma &= \zeta + \zeta^{-1} \\ \sigma^2 &= \zeta^2 + 2 + \zeta^{-2} \\ \zeta^3 &= \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} \\ \zeta^4 &= \zeta^4 + 4\zeta^2 + 6 + 4\zeta^{-2} + \zeta^{-4}, \end{aligned}$$

so

$$\begin{aligned} \rho &= \sigma^4 - \sigma^3 - 4\sigma^2 + 4\sigma + 1 \\ &= (\zeta^4 + 4\zeta^2 + 6 + 4\zeta^{-2} + \zeta^{-4}) - (\zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3}) \\ &\quad - (4\zeta^2 + 8 + 4\zeta^{-2}) + (4\zeta + 4\zeta^{-1}) + 1 \\ &= \zeta^4 - \zeta^3 + \zeta - 1 + \zeta^{-1} - \zeta^{-3} + \zeta^{-4}. \end{aligned}$$

It follows that

$$\begin{aligned} (\sigma+1)\rho &= \zeta\rho + \rho + \zeta^{-1}\rho \\ &= \zeta^5 - \zeta^4 + \zeta^2 - \zeta + 1 - \zeta^{-2} + \zeta^{-3} + \\ &\qquad \zeta^4 - \zeta^3 + \zeta - 1 + \zeta^{-1} - \zeta^{-3} + \zeta^{-4} + \\ &\qquad \zeta^3 - \zeta^2 + 1 - \zeta^{-1} + 1 - \zeta^{-4} + \zeta^{-5} \\ &= \zeta^5 + 1 + \zeta^{-5}, \end{aligned}$$

and thus that

$$\begin{aligned} (\zeta^5-1)\zeta^5(\sigma+1)\rho &= (\zeta^5-1)(\zeta^{10} + \zeta^5 + 1) \\ &= \zeta^{15} + \zeta^{10} + \zeta^5 - \zeta^{10} - \zeta^5 - 1 \\ &= \zeta^{15} - 1 = e^{2\pi i} - 1 = 0. \end{aligned}$$

We have $\zeta = \cos(2\pi/15) + i\sin(2\pi/15)$ so $\sigma = 2\cos(2\pi/15)$. It is well-known that $\cos(\theta) > 0$ for $|\theta| < \pi/2$ and $2\pi/15 < \pi/2$ so $\sigma > 0$. This implies that $\sigma + 1 \neq 0$. We also have $\zeta^5 = e^{2\pi i/3} = (-1+\sqrt{3}i)/2 \neq 1$ so $\zeta^5 - 1 \neq 0$ and clearly also $\zeta^5 \neq 0$. As $(\zeta^5-1)\zeta^5(\sigma+1)\rho = 0$ and the numbers $\zeta^5 - 1$, ζ^5 and $\sigma + 1$ are all nonzero we must have $\rho = 0$.

Next, we have

$$\begin{aligned} q_0(t)q_1(t) &= (t^2 - \tau t + \tau^{-1} - 1)(t^2 + \tau^{-1}t - \tau - 1) \\ &= t^4 + (\tau^{-1} - \tau)t^3 + (-\tau - 1 - \tau\tau^{-1} + \tau^{-1} - 1)t^2 + (\tau(\tau+1) + (\tau^{-1} - 1)\tau^{-1})t - (\tau^{-1} - 1)(\tau + 1) \\ &= t^4 - (\tau - \tau^{-1})t^3 - (\tau - \tau^{-1} + 3)t^2 + (\tau^2 + \tau^{-2} + \tau - \tau^{-1})t + (\tau - \tau^{-1}). \end{aligned}$$

We can simplify most of the terms using the fact that $\tau - \tau^{-1} = 1$. To simplify the coefficient of t we square this equation to get $\tau^2 - 2 + \tau^{-2} = 1$ and thus $\tau^2 + \tau^{-2} = 3$. Putting this all in we get

$$\begin{aligned} q_0(t)q_1(t) &= t^4 - t^3 - (1+3)t^2 + (3+1)t + 1 \\ &= t^4 - t^3 - 4t^2 + 4t + 1, \end{aligned}$$

as claimed. This implies that $0 = \rho = \sigma^4 - \sigma^3 - 4\sigma^2 + 4\sigma + 1 = q_0(\sigma)q_1(\sigma)$, so either $q_0(\sigma)$ or $q_1(\sigma)$ is zero. We are given that $q_1(\sigma) \neq 0$ so $q_0(\sigma) = 0$. The roots of the equation $q_0(t) = 0$ are $t = (\tau \pm \sqrt{\tau^2 - 4\tau^{-1} + 4})/2$. We have $\tau^2 = \tau + 1$ and $\tau^{-1} = \tau - 1$ so $\tau^2 - 4\tau^{-1} + 4 = \tau + 1 - 4\tau + 4 + 4 = 9 - 3\tau$. Thus the roots are $t = (\tau \pm \sqrt{9 - 3\tau})/2$. We have $\tau = (1 + \sqrt{5})/2 \simeq 1.618$ and so $\sqrt{9 - 3\tau} \simeq 2.036$, so $(\tau - \sqrt{9 - 3\tau})/2 < 0$. As σ is a positive root of q_0 we must have $\sigma = (\tau + \sqrt{9 - 3\tau})/2$.

Exercise 31. Show that the centre of S_n is trivial, for $n \geq 3$.

Solution:

Exercise 32. The group Dir(Cube) of rotational symmetries of the cube acts on the surface of the cube. Find the sizes of the orbits of points on the surface and describe geometrically which points have which orbit sizes.

Solution: Let S be the surface of the cube. For any point $x \in S$ we have $|Gx| = |G|/|\text{stab}_G(x)| = 24/|\text{stab}_G(x)|$. Moreover, $\text{stab}_G(x)$ is the group of all rotations around x that preserve the cube. For most points x there are no such rotations (except for the identity) and so $|\text{stab}_G(x)| = 1$ and the orbit Gx has order 24. If x is the centre of a face then $\text{stab}_G(x)$ is cyclic of order 4 and so $|Gx| = 24/4 = 6$. In fact, Gx consists of the centres of the 6 faces. If x is a vertex of the cube then $\text{stab}_G(x)$ is cyclic of order 3 and so $|Gx| = 24/3 = 8$. In fact, in this case Gx consists of the 8 vertices of the cube. If x is the midpoint of an edge then $\text{stab}_G(x)$ has order 2 and so $|Gx| = 24/2 = 12$. In fact, in this case Gx consists of the midpoints of the 12 edges of the cube. In all other cases we have $|Gx| = 24$.

Exercise 33. Show that if $S \in$ Symm(Cube) is a reflection then $S = -R$ for some rotation $R \in$ Dir(Cube) of order 2. Conversely, show that if $R \in$ Dir(Cube) is a rotation of order 2 then $-R \in$ Symm(Cube) is a reflection. Hence find how many reflections there in Symm(Cube).

Solution:

Exercise 34. (a) Show that if G is a group of order p^n for some n then the centre of G is non-trivial.

(b) Show that any group of order p^2 is abelian. [Hint: consider $G/Z(G)$]

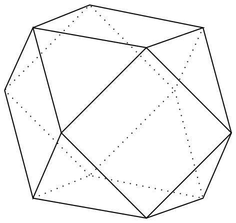
(c) Conclude that any group of order p^2 is either cyclic or isomorphic to $C_p \times C_p$.

Solution:

Exercise 35. Show that if G is a semidirect product of H and K with H and K *both* normal then in fact $G \simeq H \times K$.

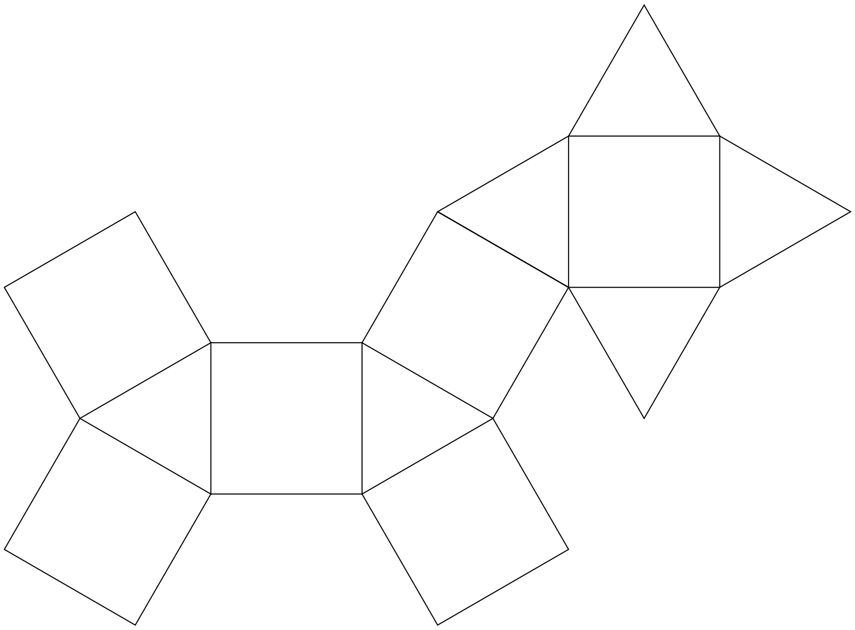
Solution:

Exercise 36. The following diagram shows a cuboctahedron X in $\mathbb{R}^3$, centred at the origin. Its faces are squares and equilateral triangles.



Which of the standard finite subgroups of SO_3 is isomorphic to Dir(X)? What can you deduce about Symm(X)?

You may wish to make a model from the net below.



Solution: Put $G = \mathrm{Dir}(X)$, which is a finite subgroup of SO_3. The normalisations of the midpoints of the edges are poles of degree 2, the normalisations of the centres of the triangular faces are poles of degree 3, and the normalisations of the centres of the square faces are poles of degree 4. The only one of the standard groups that has poles of degrees 2, 3 and 4 is G_2, so G must be conjugate to G_2 and thus isomorphic to S_4.

One can see from the picture that multiplication by -1 preserves X and so Proposition 6.9 in the notes tells us that $\mathrm{Symm}(X) \simeq \{\pm 1\} \times \mathrm{Dir}(X) \simeq \{\pm 1\} \times S_4$.

Exercise 37. Let $g\colon \mathbb{R}^3 \to \mathbb{R}^3$ be the map $g(x, y, z) = (y, z, x)$.

(a) Prove that $g \in O_3$.
(b) Find a unit vector u with $g(u) = u$.
(c) Find the order of g and deduce that $g \in SO_3$.
(d) Show that g preserves the standard cube (with centre at the origin and edges of length 2 parallel to the x, y and z axes).
(e) Describe the effect of g geometrically.

Solution:

(a) It is clear that g is linear, and we have
$$\|g(x, y, z)\|^2 = y^2 + z^2 + x^2 = x^2 + y^2 + z^2 = \|(x, y, z)\|^2,$$
so g preserves lengths. Thus $g \in O_3$.
(b) Visibly $g(a, a, a) = (a, a, a)$ for any a. To get a unit vector, put $a = 1/\sqrt{3}$.
(c) We have $g^2(x, y, z) = g(y, z, x) = (z, x, y)$ and $g^3(x, y, z) = g(z, x, y) = (x, y, z)$, so $g^3 = 1$ and g has order 3. Because $g \in O_3$ we have $\det(g) = \pm 1$ and $\det(g)^3 = \det(g^3) = \det(1) = 1$ which would give a contradiction if $\det(g)$ were -1, so $\det(g) = 1$. Thus $g \in SO_3$.
(d) The vertices of the standard cube are the points (x, y, z) for which $x, y, z \in \{1, -1\}$. Clearly, if (x, y, z) satisfies this condition then so does (y, z, x), so g carries vertices of the cube to vertices of the cube, so it sends the cube to itself.
(e) As $g \in SO_3$, it must be a rotation. Part (b) shows that the axis of rotation is the line $x = y = z$. Part (c) implies that the angle of rotation is $2\pi/3$. As $g(0, 0, 1) = (0, 1, 0)$ we see that g carries the z-axis to the y-axis and thus that the direction of rotation (as seen while looking from $(1, 1, 1)$ towards the origin) is clockwise.

Exercise 38. Let M_1, M_2 and M_3 be the x, y and z-axes.

(a) Use these to define a homomorphism $\psi\colon \mathrm{Dir}(\mathrm{Cube}) \to S_3$.

(b) Describe some elements $g \in \mathrm{Dir}(\mathrm{Cube})$ and the corresponding permutations $\psi(g)$.
(c) Show that ψ is surjective.
(d) Show that the kernel of ψ is isomorphic to $C_2 \times C_2$.

Solution:

(a) For any $g \in \mathrm{Dir}(\mathrm{Cube})$ we let $\psi(g)$ be the permutation such that $g(M_i) = M_{\sigma(i)}$ for $i = 1, 2, 3$.

(b) Let g be a half turn around the vector $(0, 1, 1)$, let h be a one-third turn anticlockwise about the vector $(1, 1, 1)$, and let k be a quarter turn anticlockwise about the vector $(0, 0, 1)$. Then $\psi(g) = (2\ 3)$, $\psi(h) = (1\ 2\ 3)$ and $\psi(k) = (1\ 2)$.

(c) Part (b) shows that the image of ψ contains $(1\ 2)$ and $(2\ 3)$, and these two transpositions generate S_3 so ψ is surjective. More explicitly, we have

$$\begin{array}{ll} \psi(1) = 1 & \psi(k) = (1\ 2) \\ \psi(h) = (1\ 2\ 3) & \psi(g) = (2\ 3) \\ \psi(h^{-1}) = (1\ 3\ 2) & \psi(gh) = (1\ 3). \end{array}$$

(d) Let G be the group of matrices of the form

$$g = \begin{pmatrix} \epsilon_1 & 0 & 0 \\ 0 & \epsilon_2 & 0 \\ 0 & 0 & \epsilon_3 \end{pmatrix}$$

such that $\epsilon_1\epsilon_2\epsilon_3 = 1$. It is easy to see that G is a subgroup of SO_3 and that it preserves the cube so it is a subgroup of $\mathrm{Dir}(\mathrm{Cube})$. If $g \in G$ and $x \in \mathbb{R}$ then $g(x, 0, 0) = (\pm x, 0, 0)$, so g preserves the x-axis, or in other words $g(M_1) = M_1$. Similarly, we have $g(M_2) = M_2$ and $g(M_3) = M_3$, so $\psi(g) = 1$, so $G \leq \ker(\psi)$.

Conversely, if $g \in \ker(\psi)$ then $g(M_1) = M_1$. The axis M_1 meets the surface of the cube at $(1, 0, 0)$ and $(-1, 0, 0)$, so $g(1, 0, 0) = \epsilon_1(1, 0, 0)$ for some $\epsilon_1 \in \{1, -1\}$. Similarly we have $g(0, 1, 0) = \epsilon_2(0, 1, 0)$ and $g(0, 0, 1) = \epsilon_3(0, 0, 1)$ for some $\epsilon_2, \epsilon_3 \in \{1, -1\}$. Thus, the matrix of g has the form described above, and as $g \in \mathrm{Dir}(\mathrm{Cube}) \leq SO_3$ we have $\det(g) = 1$ so $\epsilon_1\epsilon_2\epsilon_3 = 1$ so $g \in G$. This shows that $\ker(\psi) = G$.

We can define an isomorphism $\chi\colon C_2 \times C_2 = \{\pm 1\} \times \{\pm 1\} \to G$ by $\chi(\epsilon_1, \epsilon_2) = (\epsilon_1, \epsilon_2, \epsilon_1\epsilon_2)$.

Exercise 39. Consider the action of G on $\mathcal{C}$ as in Question 1. Observe that the stabilizer of H is

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

This is called the *normalizer* of H in G.

(a) (i) Show that H is a normal subgroup of $N_G(H)$.
(ii) Show that if H is normal in K then $K \subseteq N_G(H)$.

(b) Consider the action of H on the set G/H of left cosets of H by left translation: $h * (gH) = hgH$.
(i) Show that $\{kH\}$ is a complete orbit if and only if $k^{-1}Hk = H$.
(ii) Let w be the number of singleton orbits. Show that if H is a p-group then

$$[G : H] \equiv w \pmod{p}.$$

(iii) Conclude that if G is a p-group and $H \neq G$ then $H \neq N_G(H)$.
(iv) Deduce from (iii) that if G is a p-group and H is a subgroup of index p then H is normal in G.

Solution:

Exercise 40. Let G be a group of order 77, and let X be a set of order 96 on which G acts. Suppose there are precisely four orbits. By investigating the possible sizes of the orbits, show that there is exactly one point $x \in X$ such that $gx = x$ for all $g \in G$.

Solution: Let the sizes of the 4 orbits be d_1, d_2, d_3 and d_4 with $d_1 \leq d_2 \leq d_3 \leq d_4$. These sizes must divide 77, and thus must be 1, 7, 11 or 77. We must also have $d_1 + d_2 + d_3 + d_4 = 96$. If $d_4 \neq 77$ then $d_i \leq 11$ for all i so $96 = d_1 + d_2 + d_3 + d_4 \leq 4 \times 11 = 44$, which is false. Thus $d_4 = 77$ and $d_1 + d_2 + d_3 = 96 - 77 = 19$. By similar arguments or by inspection we must have $d_1 = 1$, $d_2 = 7$ and $d_3 = 11$. Thus, there is precisely one orbit of size 1. If this orbit has the form $\{x\}$ then x is fixed under the action of G. If y is in any of the other orbits then $|Gy| > 1$ so y is not fixed. Thus, there is precisely one fixed point.

Exercise 41. Let G be a finite group, and let X be a set with an action of G. Suppose that there is precisely one orbit, and that $|X| > 1$. Use the orbit counting theorem to show that there is an element $g \in G$ such that $\text{Fix}(g) = \emptyset$.

Solution: The identity element fixes all of X, so it has more than one fixed point. The orbit counting theorem says that the average number of fixed points is the number of orbits, which is 1. As the identity has more than one fixed point, some other element $g \in G$ must have less than one, so as to bring the average back down to 1. Thus $|\text{Fix}(g)| < 1$ but of course $|\text{Fix}(g)|$ is a nonnegative integer so $|\text{Fix}(g)| = 0$ so $\text{Fix}(g) = \emptyset$.

For a more algebraic presentation, note that $\sum_{g\in G} 1 = |G|$, so $|G|^{-1}\sum_{g\in G} 1 = 1$. The orbit counting theorem tells us that $|G|^{-1}\sum_{g\in G}|\text{Fix}(g)| = \text{ number of orbits } = 1$. By subtracting these equations we find that $\sum_{g\in G}(|\text{Fix}(g)|-1) = 0$. If we move the $g = 1$ term to the other side we get $\sum_{g\neq 1}(|\text{Fix}(g)|-1) = 1-|X|$. The right hand side is less than 0, so at least one of the terms on the left must be less than 0, so $|\text{Fix}(g)|-1 < 0$ for some g. As before, this means that $\text{Fix}(g) = \emptyset$.

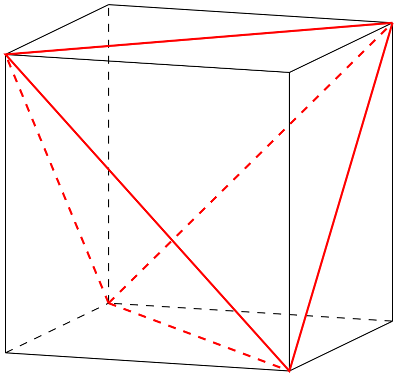
Exercise 42. Let G be a finite simple group (so there are no normal subgroups of G except for $\{1\}$ and G itself). Let p be a prime dividing the order of G, and let X be a set of order n on which the group acts. Suppose that the action is nontrivial, so there is and element $g \in G$ and an element $x \in X$ such that $gx \neq x$. Prove that $n \geq p$.

[**Hint:** Use X to define a homomorphism and consider its kernel. For which integers m does p divide $m!$?]

Solution: We can use X to define a homomorphism $G \to S_n$ in the usual way. (In other words, we list the elements of X as $\{x_1, \dots, x_n\}$ say, and then let $\phi(g)$ be the permutation σ such that $gx_i = x_{\sigma(i)}$ for all i.) The kernel of any homomorphism is a normal subgroup, and there are only two normal subgroups of G so either $\ker(\phi) = \{1\}$ or $\ker(\phi) = G$. As the action is nontrivial, we have $gx_i \neq x_i$ for some $g \in G$ and $i \in \{1, \dots, n\}$, so $\phi(g)(i) \neq i$, so $\phi(g) \neq 1$. Thus $g \notin \ker(\phi)$, so $\ker(\phi) \neq G$, so we must have $\ker(\phi) = \{1\}$. This means that ϕ is injective and thus that $|G| = |\phi(G)|$. Moreover, $\phi(G)$ is a subgroup of S_n, so $n! = |S_n|$ is divisible by $|\phi(G)| = |G|$, and $|G|$ is divisible by p, so $n!$ is divisible by p. Now, if $m < p$ then none of the numbers $1, 2, \dots, m$ are divisible by p so $m!$ is not divisible by p. As p divides $n!$ we must have $n \geq p$ as claimed.

Exercise 43. We know that $\text{Dir(Tet)} \simeq A_4$ and that $\text{Dir(Cube)} \simeq S_4$. Find a geometric reason that Dir(Tet) is isomorphic to a subgroup of Dir(Cube). [Hint: can you see a tetrahedron inside the cube?]

Solution: The following picture shows a tetrahedron embedded inside a cube. We'll assume as usual that the edges of the cube have length 2.



Alternatively, we can say that the cube is built from the tetrahedron by attaching a pyramid to each face. All the pyramids have the same shape: the base edges have length $2\sqrt{2}$, and the remaining edges have length 2. Thus, any isometry of the tetrahedron carries pyramids to pyramids and thus gives an isometry of the cube. This shows that $\text{Dir(Tet)} \leq \text{Dir(Cube)}$.

Exercise 44. In this problem we will find the coordinates of the vertices of a tetrahedron. We will place the tetrahedron with its centre at the origin and the first vertex v_1 on the z-axis. After choosing suitable units of length we may assume that $v_1 = (0, 0, \sqrt{3})$. We then rotate our coordinates if necessary so that the next vertex v_2 lies in the xz-plane, say $v_2 = (a, 0, -b)$. There are two more vertices; we call the one with positive y-coordinate v_3, and the one with negative y-coordinate v_4.

(a) Explain why the points v_3 and v_4 lie in the plane $z = -b$.
(b) Explain why $v_3 = (-a/2, a\sqrt{3}/2, -b)$, and give the corresponding formula for v_4.
(c) By considering the distances $d(O, v_i)$ and $d(v_i, v_j)$ show that $a^2 + b^2 = 3$ and $a^2 + (b + \sqrt{3})^2 = 3a^2$.
(d) Solve these equations for a and b, and obtain explicit expressions for the coordinates of v_2, v_3 and v_4.
(e) Consider the matrix

$$g = \begin{pmatrix} 1/3 & 0 & \sqrt{8}/3 \\ 0 & -1 & 0 \\ \sqrt{8}/3 & 0 & -1/3 \end{pmatrix}$$

Calculate $g(v_i)$ for $i = 1, 2, 3, 4$ and thus determine the vertex permutation induced by g.

Solution:

(a) A twist of one third around the z-axis sends v_2 to v_3, v_3 to v_4 and v_4 to v_2. Such a twist preserves horizontal planes, and v_2 lies in the plane $z = -b$ so the same is true of v_3 and v_4.
(b) Let w_2, w_3 and w_4 be the points in the xy plane lying above v_2, v_3 and v_4. Then $w_2 = (a, 0)$ and w_3 and w_4 are obtained from w_2 by rotating around the origin through $2\pi/3$ in either direction, so the coordinates are $(\cos(\pm 2\pi/3)a, \sin(\pm 2\pi/3)a)$, which is equal to $(-a/2, \pm a\sqrt{3}/2)$. In combination with (a) this means that $v_3 = (-a/2, a\sqrt{3}/2, -b)$ and $v_3 = (-a/2, -a\sqrt{3}/2, -b)$.
(c) All the vertices of a tetrahedron have the same distance from the centre, so $\|v_2\|^2 = \|v_1\|^2$, or in other words $a^2 + b^2 = 3$. The distance between any two vertices is the same, so $d(v_1, v_2) = d(v_3, v_4)$. We have $v_1 - v_2 = (-a, 0, b + \sqrt{3})$ so $d(v_1, v_2)^2 = a^2 + (b + \sqrt{3})^2$. We also have $v_2 - v_3 = (0, a\sqrt{3}, 0)$, so $d(v_2, v_3)^2 = 3a^2$. It follows that $a^2 + (b + \sqrt{3})^2 = 3a^2$ as claimed.
(d) Our second equation expands out to give $b^2 + 2b\sqrt{3} + 3 - 2a^2 = 0$. Our first equation gives $a^2 = 3 - b^2$ and after substituting this in we get $3b^2 + 2b\sqrt{3} - 3 = 0$, so $b^2 + 2b/\sqrt{3} - 1 = 0$, so $(b + 1/\sqrt{3})^2 = 4/3$. As b must clearly be positive this gives $b = 1/\sqrt{3}$. This implies that $a^2 = 3 - b^2 = 3 - 1/3 = 8/3$ so $a = \sqrt{8/3} = 2\sqrt{2/3}$. Putting this back into our equations for the v_i gives

$$\begin{aligned} v_1 &= (0, 0, \sqrt{3}) \\ v_2 &= (2\sqrt{2/3}, 0, -1/\sqrt{3}) \\ v_3 &= (-\sqrt{2/3}, \sqrt{2}, -1/\sqrt{3}) \\ v_4 &= (-\sqrt{2/3}, -\sqrt{2}, -1/\sqrt{3}). \end{aligned}$$

(e) Let V be the matrix whose columns are v_1, v_2, v_3 and v_4, so gV is the matrix whose columns are gv_1, gv_2, gv_3 and gv_4. We have

$$\begin{aligned} gV &= \begin{pmatrix} 1/3 & 0 & 2\sqrt{2}/3 \\ 0 & -1 & 0 \\ 2\sqrt{2}/3 & 0 & -1/3 \end{pmatrix} \begin{pmatrix} 0 & 2\sqrt{2/3} & -\sqrt{2/3} & -\sqrt{2/3} \\ 0 & 0 & \sqrt{2} & -\sqrt{2} \\ \sqrt{3} & -1/\sqrt{3} & -1/\sqrt{3} & -1/\sqrt{3} \end{pmatrix} \\ &= \begin{pmatrix} 2\sqrt{2/3} & 0 & -\sqrt{2/3} & -\sqrt{2/3} \\ 0 & 0 & -\sqrt{2} & \sqrt{2} \\ -1/\sqrt{3} & \sqrt{3} & -1/\sqrt{3} & -1/\sqrt{3} \end{pmatrix}, \end{aligned}$$

so $g(v_1) = v_2$, $g(v_2) = v_1$, $g(v_3) = v_4$ and $g(v_4) = v_3$. Thus, the permutation associated to g is $(1\ 2)(3\ 4)$.

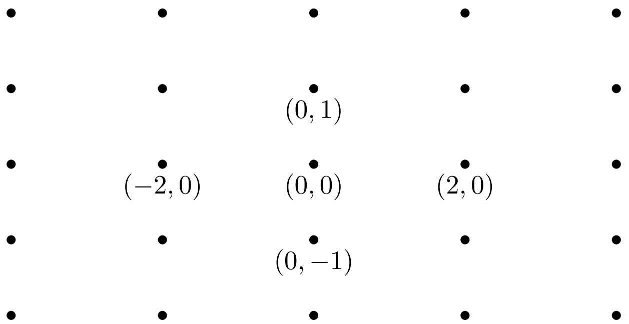
Exercise 45. Let (e_1, e_2) be the usual basis of $\mathbb{R}^2$, let $L = \Re_1$ be the x-axis and $S = S_e$.

Show that if G is the subgroup $\langle ST_1, T_2 \rangle$ of I_2 then the point group $\psi(G)$ is cyclic of order 2, whereas $\sigma_a(G)$ is trivial for all $a \in \mathbb{R}^2$.
[Hint: For the second part show that every $g \in G$ can be written in the form: $S^{i_1} T_1^{i_1} T_2^{i_2}$.]

Solution:

Exercise 46. Let H be a wallpaper group such that $\mathrm{Trans}(H) = \{(2n, m) \mid n, m \in \mathbb{Z}\}$. Prove that $|\psi(H)| \leq 4$.

Solution: The group $\mathrm{Trans}(H) \leq \mathbb{R}^2$ looks like this:



We know that if $A \in \psi(H)$ then $A.\mathrm{Trans}(H) = \mathrm{Trans}(H)$ (Lemma 5.8 in the notes). If A is a rotation about the origin that sends $\mathrm{Trans}(H)$ to itself, then the angle must be 0 or π, so $A = I$ or R_π. If A is the reflection across a line L through the origin, then L must be either the x-axis or the y-axis, so $A = S_0$ or S_π. Thus $\psi(H) \subseteq \{1, S_0, S_\pi, S_0S_\pi\}$ and so $|\psi(H)| \leq 4$.

Here is a slightly more formal argument. We know that $A.\mathrm{Trans}(H) = \mathrm{Trans}(H)$, so $A(0,1)$ lies in $\mathrm{Trans}(H)$ and has length 1, so $A(0,1) = (0,1)$ or $A(0,1) = (0,-1)$. In the first case we define $A_1 = A$, and in the second we define $A_1 = S_0A$; either way we have $A_1.\mathrm{Trans}(H) = \mathrm{Trans}(H)$ and $A_1(0,1) = (0,1)$. As A_1 preserves lengths and angles we see that $A_1(2,0)$ is perpendicular to $A_1(0,1) = (0,1)$ and $\|A_1(2,0)\| = 2$; the only possibilities are $A_1(2,0) = (2,0)$ or $A_1(2,0) = (-2,0)$. In the first case we put $A_2 = A_1$,and in the second we define $A_2 = S_\pi A_1$; either way we have $A_2(0,1) = (0,1)$ and $A_2(2,0) = (2,0)$. As $(0,1)$ and $(2,0)$ are a basis of $\mathbb{R}^2$, this means that $A_2 = 1$, and it follows that A is either 1, S_0, S_π or $S_0S_\pi = R_\pi$.

Exercise 47. Let Oct be a regular octahedron, centred at the origin in $\mathbb{R}^3$. Since Oct is dual to the cube we know that $\mathrm{Dir}(\mathrm{Oct}) \simeq S_4$. Prove this directly as follows:

(i) Describe 24 rotation in Dir(Oct).

(ii) Describe a set of 4 objects in which Dir(Oct) acts and such that the induced homorphism $\mathrm{Dir}(\mathrm{Oct}) \to S_4$ is injective. Prove your assertions.

Solution:

Exercise 48. By considering cycle types show that A_5 has no elements of order 15. What does the classification of finite subgroups of SO_3 tell us about subgroups of A_5 of order 30? Show that there are no such subgroups.

Solution: A_5 consists of elements of the following types:

- the identity, with order 1
- transposition pairs (such as (1 2)(3 4)), with order 2
- 3-cycles (such as (1 2 3)), with order 3
- 5-cycles (such as (1 2 3 4 5)) with order 5.

There are thus no elements of order 15.

Now let G be a subgroup of A_5 with $|G| = 30$. The group A_5 is isomorphic to the subgroup G_3 of SO_3, so G is isomorphic to some subgroup of G_3 and thus to a finite subgroup of SO_3. It follows by the classification that G is isomorphic to G_1, G_2 or G_3, or to $\widetilde{C}_n$ or $\widetilde{D}_n$ for some n. As $|G| = 30$ which is different from the orders of G_1, G_2 and G_3 we must have $G \simeq \widetilde{C}_{30}$ or $G \simeq \widetilde{D}_{15}$. However $\widetilde{C}_{30}$ and $\widetilde{D}_{15}$ both contain elements of order 15 and G does not, which gives a contradiction. Thus there can be no subgroups of A_5 of order 30.

Exercise 49. Suppose H is a subgroup of a finite group G, and consider the action of G on the set

$$\mathcal{C} = \{gHg^{-1} \mid g \in G\}$$

of conjugates of H.

(i) Show that $h * K = hKh^{-1}$ defines an action of G on $\mathcal{C}$.

(ii) Conclude that $|\mathcal{C}|$ divides the order of G.

(iii) Suppose G is of order $p^n s$ with $(p, s) = 1$ and n_p is the number of conjugates of P. Use Part (ii) to show that if $n_p \equiv 1 \bmod p$ then n_p divides s.

Solution:

Exercise 50. Let G be a group of order 605. Show that G has a normal subgroup of order 121 and hence show that G is a semidirect product of proper subgroups.

Find a group automorphism $\theta\colon C_{11} \times C_{11} \to C_{11} \times C_{11}$ of order 5. Construct a non-abelian group of order 605 which has a subgroup isomorphic to $C_{11} \times C_{11}$ (You may use general facts about automorphism groups of elementary abelian groups without proof.)

Solution:

Exercise 51. Write out the multiplication table of the group $\mathbb{Z}_3 \rtimes_{-1} \mathbb{Z}_2$.

Solution:

	$(0,0)$	$(+1,0)$	$(-1,0)$	$(0,1)$	$(+1,1)$	$(-1,1)$
$(0,0)$	$(0,0)$	$(+1,0)$	$(-1,0)$	$(0,1)$	$(+1,1)$	$(-1,1)$
$(+1,0)$	$(+1,0)$	$(-1,0)$	$(0,0)$	$(+1,1)$	$(-1,1)$	$(0,1)$
$(-1,0)$	$(-1,0)$	$(0,0)$	$(+1,0)$	$(-1,1)$	$(0,1)$	$(+1,1)$
$(0,1)$	$(0,1)$	$(-1,1)$	$(+1,1)$	$(0,0)$	$(+1,0)$	$(-1,0)$
$(+1,1)$	$(+1,1)$	$(0,1)$	$(-1,1)$	$(+1,0)$	$(0,0)$	$(+1,0)$
$(-1,1)$	$(-1,1)$	$(+1,1)$	$(0,1)$	$(-1,0)$	$(-1,0)$	$(0,0)$

Exercise 52. Prove by induction that in $\mathbb{Z}_n \rtimes_a \mathbb{Z}_m$ we have

$$(v,w)^k = (v + a^w v + \ldots + a^{(k-1)w} v, kw).$$

List the elements of the group $G = \mathbb{Z}_5 \rtimes_2 \mathbb{Z}_4$. Calculate the element $\overline{1} + \overline{2} + \overline{2}^2 + \overline{2}^3 \in \mathbb{Z}_5$. Can you explain your result (*carefully*) with less calculation? Show that every element of G has order 1, 2, 4 or 5.

Solution: The base case says that $(v,w)^1 = (v,w)$, which is clear. Given the statement for $(v,w)^k$ we have

$$\begin{aligned} (v,w)^{k+1} &= (v,w)(v,w)^k \\ &= (v,w)(v + a^w v + \ldots + a^{(k-1)w} v, kw) \\ &= (v + a^w(v + a^w v + \ldots + a^{(k-1)w} v), w + kw) \\ &= (v + a^w v + a^{2w} v + \ldots + a^{kw} v, (k+1)w), \end{aligned}$$

which is the required statement for $(v,w)^{k+1}$.

The elements of G are as follows:

$$\begin{array}{ccccc} (\overline{0},\overline{0}) & (\overline{1},\overline{0}) & (\overline{2},\overline{0}) & (\overline{3},\overline{0}) & (\overline{4},\overline{0}) \\ (\overline{0},\overline{1}) & (\overline{1},\overline{1}) & (\overline{2},\overline{1}) & (\overline{3},\overline{1}) & (\overline{4},\overline{1}) \\ (\overline{0},\overline{2}) & (\overline{1},\overline{2}) & (\overline{2},\overline{2}) & (\overline{3},\overline{2}) & (\overline{4},\overline{2}) \\ (\overline{0},\overline{3}) & (\overline{1},\overline{3}) & (\overline{2},\overline{3}) & (\overline{3},\overline{3}) & (\overline{4},\overline{3}). \end{array}$$

We have $\overline{2}^2 = \overline{4}$ and $\overline{2}^3 = \overline{8} = \overline{3}$ so $\overline{1} + \overline{2} + \overline{2}^2 + \overline{2}^3 = \overline{1} + \overline{2} + \overline{4} + \overline{3} = \overline{10} = \overline{0}$. Alternatively, the group $\mathbb{Z}_5^\times$ has order 4, so for any $x \in \mathbb{Z}_5^\times$ we have $x^4 = 1$ and thus $(x - \overline{1})(\overline{1} + x + x^2 + x^3) = x^4 - \overline{1} = \overline{0}$. If $x \neq \overline{1}$ then the element $x - \overline{1}$ is nonzero and thus has a multiplicative inverse in $\mathbb{Z}_5$, so we can multiply by this inverse to see that $\overline{1} + x + x^2 + x^3 = \overline{0}$. By putting $x = \overline{2}$ we see again that $\overline{1} + \overline{2} + \overline{2}^2 + \overline{2}^3 = \overline{0}$.

Now, for any element $(v,w) \in G$ we have

$$(v,w)^4 = (v + \overline{2}^w v + \overline{2}^{2w} v + \overline{2}^{3w} v, 4w) = ((\overline{1} + \overline{2}^w + \overline{2}^{2w} + \overline{2}^{3w})v, 0).$$

(Here we have used the fact that $4w = 0$ for all $w \in \mathbb{Z}_4$.) If $w \neq 0$ we can put $x = \overline{2}^w \neq 1$ in the previous paragraph and deduce that $\overline{1} + \overline{2}^w + \overline{2}^{2w} + \overline{2}^{3w} = \overline{0}$, so $(v,w)^4 = (0,0)$, which implies that the order of (v,w) is 1, 2 or 4. On the other hand, if $w = 0$ then it is easy to see that $(v,w)^k = (v,0)^k = (kv,0)$ and thus that $(v,w)^5 = (0,0)$, so the order of (v,w) is 1 or 5.

Exercise 53. Recall that if H and K are groups the Cartesian product $H \times K$ is a group under the operation $(h, k)(h', k') = (hh', kk')$.

Show that if G is a group and $a, b \in G$ are distinct with the property that a, b and ab all have order 2 then $L = \{e, a, b, ab\}$ is a subgroup of G and L is isomorphic to $C_2 \times C_2$.

Show that if K is any group of order 4 then either $K \simeq C_4$ or $K \simeq C_2 \times C_2$, but not both. Which of these two alternatives hold for $K = D_2$?

Solution: We first claim that the elements e, a, b and ab are all distinct. Indeed, if $a = e$ or $b = e$ or $ab = e$ then a, b or ab would have order 1 rather than 2, contradicting our assumption. We also have $b \neq a$ by assumption. We cannot have $ab = a$, because if we did we could multiply on the left by a^{-1} to get $b = e$. Similarly, we cannot have $ab = b$, so all four elements are distinct, so L is a set of order 4.

The set L clearly contains e. As $a^2 = b^2 = (ab)^2 = e$ we have $a^{-1} = a$, $b^{-1} = b$, $(ab)^{-1} = ab$ and of course $e^{-1} = e$; thus L is closed under taking inverses. We also have $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ so a and b commute. Using this, it is easy to fill in the multiplication table as follows:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

(For example, $(ab)a = aba = aab = b$, which explains the entry in the row marked ab and the column marked a.) The table shows that L is closed under multiplication, so it is a subgroup. Recall that $C_2 = \{1, R\}$ where $R^2 = 1$. We can define $\phi\colon C_2 \times C_2 \to L$ by $\phi((R^i, R^j)) = a^i b^j$, so

$$\begin{aligned} \phi((1,1)) &= e \\ \phi((R,1)) &= a \\ \phi((1,R)) &= b \\ \phi((R,R)) &= ab \end{aligned}$$

As $C_2 \times C_2 = \{(1,1), (R,1), (1,R), (R,R)\}$ we see that ϕ is a bijection.

As a and b commute we have

$$\begin{aligned} \phi((R^i, R^j))\phi((R^k, R^l)) &= a^i b^j a^k b^l \\ &= a^i a^k b^j b^l \\ &= a^{i+k} b^{j+l} \\ &= \phi((R^{i+k}, R^{j+l})) \\ &= \phi((R^i, R^j)(R^k, R^l)), \end{aligned}$$

which shows that ϕ is a homomorphism and thus an isomorphism.

Now let K be a group of order 4. By Lagrange's theorem, every element $a \in K$ has order dividing 4 and thus equal to 1, 2 or 4. Only the identity element can have order 1 so the other 3 elements must have order 2 or 4. If there are no elements of order 4 then let a and b be any two distinct elements of order 2. Then ab is another element of K, which is not the identity because $a \neq b^{-1} = b$, so it must also have order 2. Using the first part of the question we deduce that $L = \{1, a, b, ab\}$ is a subgroup of K and is isomorphic to $C_2 \times C_2$. As $|L| = |K| = 4$ we must have $L = K$, so $K \simeq C_2 \times C_2$.

On the other hand, suppose that not all elements of $K \setminus \{1\}$ have order 2. Let a be an element of order 4, and put $L = \{1, a, a^2, a^3\}$. It is easy to see that L is a subgroup isomorphic to C_4, and $|L| = |K| = 4$ so $L = K$, so $K \simeq C_4$ as claimed.

We cannot have both $K \simeq C_2 \times C_2$ and $K \simeq C_4$, for in the first case all elements of K have order 2 whereas in the second case some elements have order 4.

Exercise 54. Let G be a group of order 18.

(a) Show that there is a normal subgroup $P \leq G$ with $|P| = 9$, and another subgroup $Q \leq G$ of the form $Q = \{1, h\}$ with $h^2 = 1$ (and so $h^{-1} = h$).

(b) Show that if $P \simeq C_9$ then $G \simeq C_2 \times C_9$ or $G \simeq D_9$.

(c) Now suppose that $P \simeq C_3 \times C_3$ (so in particular, P is abelian, and $x^3 = 1$ for all $x \in P$). For any $x \in P$, we put

$$\begin{aligned} x^h &= hxh = h^{-1}xh \\ x_+ &= x^2\,(x^h)^2 = xxhxhhxh = xxhxxh \\ x_- &= x^2\,x^h = xxhxh \\ P_+ &= \{x \in P \mid x^h = x\} \\ P_- &= \{x \in P \mid x^h = x^{-1}\}. \end{aligned}$$

(i) Show that $x_+ \in P_+$ and $x_- \in P_-$ and $x = x_+x_-$.

(ii) Show that P_+ and P_- are subgroups of P, and that $P_+ \cap P_- = \{1\}$.

(iii) Deduce that $P \simeq P_+ \times P_-$.

(iv) Show that if $|P_+| = 9$ then $G \simeq C_3 \times C_3 \times C_2$.

(v) Show that if $|P_+| = 3$ then $G \simeq C_3 \times D_3$.

(The case $|P_+| = 1$ gives a new group, for which we do not yet have a name.)

Solution:

(a) We know that n_3 divides 2 and is congruent to 1 modulo 3; the only possibility is $n_3 = 1$. This means that there is a unique, normal Sylow 3-subgroup, which we call P. We then let Q be any Sylow 2-subgroup. As $|Q| = 2$, it is clear that $Q = \{1, h\}$ for some h with $h^2 = 1$.

(b) Suppose that $P \simeq C_9$. We can then choose an element $g \in P$ that generates P, with $g^9 = 1$. As P is normal, we see that $hgh = g^a$ for some integer a. As $h^2 = 1$, this means that

$$g = h^2gh^2 = hg^ah = g^{a^2},$$

so $a^2 = 1 \pmod 9$, so the number $a^2 - 1 = (a+1)(a-1)$ is divisible by 9. The following table shows all numbers a mod 9 and their squares:

a	-4	-3	-2	-1	0	1	2	3	4
a^2	-2	0	4	1	0	1	4	0	-2

As $a^2 = 1 \pmod 9$, we must have $a = 1 \pmod 9$ or $a = -1 \pmod 9$, so $hgh = g$ or $hgh = g^{-1}$. If $hgh = g$ then h commutes with g and we find that $G \simeq P \times Q \simeq C_2 \times C_9$. If $hgh = g^{-1}$ we find that $G \simeq D_9$.

(c) Now suppose instead that $P \simeq C_3 \times C_3$.

(i) We have

$$(x_+)^h = hx_+h = h(xxhxxh)h = hxxhxx.$$

Now, xx lies in P and P is normal so $hxxh$ lies in P. Moreover, P is abelian, so xx commutes with $hxxh$. We thus have $hxxhxx = xxhxxh$, or in other words, $(x_+)^h = x_+$. This shows that $x_+ \in P_+$.

Next, we have $xxx = x^3 = 1$ and so

$$(x_-)^h x_- = h(xxhxh)h\,xxhxh = hxxhxxxhxh = hxxhhxh = hxxxh = hh = 1,$$

so $(x_-)^h = (x_-)^{-1}$, so $x_- \in P_-$.

Finally, we have

$$x_+x_- = (xx)(hxxh)\,(xx)(hxh) = (xx)(xx)(hxxh)(hxh) = xhxxxh = xhh = x.$$

(In the second equality, we used the fact that each of the four bracketed terms lies in P, so we can commute them past each other.)

(ii) Clearly $1 \in P_+$ and $1 \in P_-$. If $x, y \in P_+$ we have $x = hxh$ and $y = hyh$, so $xy = hxh\,hyh = hxyh$, so $xy \in P_+$. In particular, we can take $y = x$ to see that the element $x^{-1} = x^2$ lies in P_+. This shows that P_+ is a subgroup of P. Now suppose instead that $x, y \in P_-$, so that $hxh = x^{-1}$ and $hyh = y^{-1}$. As x and y commute we have $x^{-1}y^{-1} = (xy)^{-1}$, so $hxyh = hxh\,hyh = x^{-1}y^{-1} = (xy)^{-1}$, so $xy \in P_-$. It follows that P_- is also a subgroup.

If $x \in P_+ \cap P_-$ then $x^h = x$ and also $x^h = x^{-1}$, so $x = x^{-1}$, so $x^2 = 1$. As $P \simeq C_3 \times C_3$ we also know that $x^3 = 1$, and it follows that $x = x^3(x^2)^{-1} = 1$. This shows that $P_+ \cap P_- = \{1\}$.

(iii) As P_+ and P_- are subgroups of the abelian group P, we see that they commute with each other, so we can define a homomorphism $\phi\colon P_+ \times P_- \to P$ by $\phi(y, z) = yz$. For any $x \in P$ we have $(x_+, x_-) \in P_+ \times P_-$ and $\phi(x_+, x_-) = x_+x_- = x$. This shows that ϕ is surjective. We also have $P_+ \cap P_- = \{1\}$, which implies that ϕ is injective. This means we have an isomorphism $P_+ \times P_- \to P$, and so $|P_+||P_-| = 9$.

(iv) Suppose that $|P_+| = 9$, so $P_+ = P$ and $P_- = \{1\}$. This means that $hxh = x$ for all $x \in P$, so P commutes with Q, so $G \simeq Q \times P \simeq C_2 \times C_3 \times C_3$.

(v) Now suppose instead that $|P_+| = 3$, so $|P_-| = 3$ also. This means that $P_+ \simeq P_- \simeq C_3$, so we can choose $a \in P_+$ and $b \in P_-$ such that $P_+ = \{1, a, a^2\}$ and $P_- = \{1, b, b^2\}$ and $a^3 = b^3 = 1$. We define $\phi\colon C_3 \times D_6 \to G$ by

$$\phi((R^i, R^j)) = a^i b^j$$
$$\phi((R^i, R^j S)) = a^i b^j h.$$

It is easy to check that this is an isomorphism of groups.

Exercise 55. (a) Let G be a group of order 21. Show that G has a normal subgroup of order 7 and hence show that G is a semidirect product of proper subgroups.

(b) Construct a non-abelian group of order 21.

(c) Using the fact that $\mathbb{Z}_7^\times$ is cyclic, show that every non-Abelian group of order 21 is isomorphic to the one in (b).

Solution:

(a) If we let n_7 be the number of Sylow 7-subgroups then n_7 divides 3 and is congruent to 1 modulo 7 so we must have $n_7 = 1$. If we let N be the unique Sylow 7-subgroup then it follows that N is normal in G. [Explicitly, if $g \in G$ then gNg^{-1} is clearly a subgroup of order 7 but we have seen that N is the only such subgroup so $gNg^{-1} = N$, which means that N is normal.] Now let Q be a Sylow 3-subgroup of G. The order of $N \cap Q$ divides both $7 = |N|$ and $3 = |Q|$ so we must have $|N \cap Q| = 1$ so $N \cap Q = \{1\}$. This means that $|NQ| = |N||Q|/|N \cap Q| = 21 = |G|$ so $NQ = G$, so G is the semidirect product of N and Q.

(b) Recall that $\mathbb{Z}_n \rtimes_a \mathbb{Z}_m$ is defined whenever $a \in \mathbb{Z}_n^\times$ and $a^m = \overline{1}$. As $\overline{2} \in \mathbb{Z}_7^\times$ and $\overline{2}^3 = \overline{8} = \overline{1}$, we can define the group $H = \mathbb{Z}_7 \rtimes_2 \mathbb{Z}_3$, which is a non-Abelian group of order 21.

(c) Let G be a non-Abelian group of order 21. As in part (a) we see that there are subgroups N and Q of G such that N is normal, $|N| = 7$, $|Q| = 3$, and G is the semidirect product of N and Q. As the orders of N and Q are prime, they must be cyclic groups. We saw in lectures that all semidirect products of cyclic groups have the form $\mathbb{Z}_n \rtimes_a \mathbb{Z}_m$, so $G \simeq \mathbb{Z}_7 \rtimes_a \mathbb{Z}_3$ for some $a \in \mathbb{Z}_7^\times$ with $a^3 = 1$.

We know that $\mathbb{Z}_7^\times$ is cyclic of order 6, generated by some element b say. From this it is not hard to see that there are precisely three elements satisfying $a^3 = \overline{1}$, viz. $a = \overline{1}$, $a = b^2$ and $a = b^{-2}$. Explicitly, we have

a	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{-1}$	$\overline{-2}$	$\overline{-3}$
a^3	$\overline{1}$	$\overline{1}$	$\overline{-1}$	$\overline{-1}$	$\overline{-1}$	$\overline{1}$

so the three possibilities are $a = \overline{1}$, $a = \overline{2}$ and $a = \overline{-3} = \overline{2}^{-1}$. [If we take $b = \overline{3}$ then b generates $\mathbb{Z}_7^\times$ and $b^2 = \overline{2}$ and $b^{-2} = \overline{-3}$.] The case $a = 1$ would give the Abelian group $\mathbb{Z}_7 \times \mathbb{Z}_3$, which is impossible as G is assumed to be non-Abelian.

We now see that G is isomorphic either to the group $H = \mathbb{Z}_7 \rtimes_2 \mathbb{Z}_3$ considered in part (b), or to the group $H' := \mathbb{Z}_7 \rtimes_{-3} \mathbb{Z}_3$. It will thus be enough to show that H' is isomorphic to H.

Define $\phi\colon H \to H'$ by $\phi(v, w) = (v, -w)$; this is clearly a bijection. We next show that ϕ is a homomorphism. We will write $*$ for the group operation in H and $*'$ for the group operation in H', so as to make clear which is which. We have

$$\begin{aligned}\phi((v,w)*(x,y)) &= \phi(v+\overline{2}^{w}x, w+y)\\ &= (v+\overline{2}^{w}x, -w-y)\\ &= (v+\overline{-3}^{-w}x, -w-y)\\ &= (v,-w)*'(x,-y)\\ &= \phi(v,w)*'\phi(x,y),\end{aligned}$$

which shows that ϕ is a homomorphism as claimed, and thus an isomorphism.

Exercise 56. Let G be a group of order 60, and suppose that G has a cyclic normal subgroup N of order 12. Let Q be a Sylow 5-subgroup of G. What standard groups are N, Q and $\mathrm{Aut}(N)$ isomorphic to? Show that every homomorphism $\phi\colon Q\to\mathrm{Aut}(N)$ is trivial. Deduce that every element of Q commutes with every element of N, and thus that G is Abelian.

Solution: As N is cyclic of order 12, it is isomorphic to $\mathbb{Z}_{12}$. As $|G|=5\times12$ and 5 does not divide 12, the Sylow 5-subgroup Q must have order 5. Groups of prime order are cyclic so Q is isomorphic to $\mathbb{Z}_5$. Finally, $\mathrm{Aut}(N)\simeq\mathrm{Aut}(\mathbb{Z}_{12})\simeq\mathbb{Z}_{12}^{\times}$, and we showed in lectures that $\mathbb{Z}_{12}^{\times}=\{\overline{\pm1},\overline{\pm5}\}\simeq C_2\times C_2$, so $\mathrm{Aut}(N)\simeq C_2\times C_2$. As the order of Q is coprime to the order of $\mathrm{Aut}(N)$, we deduce that any homomorphism $\phi\colon Q\to\mathrm{Aut}(N)$ is trivial. [More explicitly, if $g\in Q$ then $g^5=1$ so $\phi(g)^5=\phi(g^5)=1$. On the other hand, for any $h\in\mathrm{Aut}(N)\simeq C_2\times C_2$ we have $h^2=1$ so $\phi(g)^2=1$. This means that $\phi(g)=\phi(g)^5(\phi(g)^2)^{-2}=1$, so ϕ is trivial.]

For any $g\in Q$ we define as usual $\gamma_g\colon N\to N$ by $\gamma_g(x)=gxg^{-1}$, so $\gamma_g\in\mathrm{Aut}(N)$. We then have a homomorphism $\phi\colon Q\to\mathrm{Aut}(N)$ given by $\phi(g)=\gamma_g$. This must be trivial, by our first paragraph. Thus $gxg^{-1}=x$ for all $g\in Q$ and $x\in N$. After multiplying on the right by g we deduce that $gx=xg$ for all g and x, so every element of Q commutes with every element of N.

Now define $\mu\colon N\times Q\to G$ by $\mu(x,g)=xg=gx$. As N and Q commute, this function is a homomorphism. The image is the subgroup NQ, and because $|N|=12$ and $|Q|=5$ are coprime we have $|NQ|=|N||Q|=60=|G|$, so $NQ=G$. It follows that μ is surjective and $|N\times Q|=|G|$ so it must also be injective and thus an isomorphism. Thus $G\simeq\mathbb{Z}_{12}\times\mathbb{Z}_5$, so G is Abelian.

Exercise 57. Show that every group of order 1225 is abelian.

Solution: First note that $1225=25\times49=5^27^2$, so we will study the Sylow 5-subgroups and 7-subgroups of G. We know that n_5 divides 49 (so $n_5\in\{1,7,49\}$) and $n_5=1\pmod 5$. As $7=2\pmod 5$ and $49=4\pmod 5$ we see that the only possibility is $n_5=1$. We therefore have a unique Sylow 5-subgroup, which we call P. Note that P is normal, and also that $|P|=5^2$, so Proposition 2.8 tells us that P is abelian.

Next, we know that n_7 divides 25 (so $n_7\in\{1,5,25\}$) and $n_7=1\pmod 7$. As $5=5\pmod 7$ and $25=4\pmod 7$, we see that n_7 must be 1. There is thus a unique Sylow 7-subgroup, which we call Q. We again see that Q is normal and abelian.

Using Proposition 2.9 in the notes, we see that $G\simeq P\times Q$. This is abelian, because P and Q are.

Exercise 58. If G is a group let $\theta_g\colon G\to G$ be defined by $\theta_g(x)=gxg^{-1}$. The group of inner automorphisms is

$$\mathrm{Inn}(G)=\{\theta_g\mid g\in G\}.$$

(i) Show that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.
(ii) Calculate $\mathrm{Aut}(G)$, $\mathrm{Inn}(G)$ and $\mathrm{Out}(G)=\mathrm{Aut}(G)/\mathrm{Inn}(G)$ in the following cases
  (a) $G=C_7$
  (b) $G=C_3\times C_3$
  (c) $G=S_3$
  (d) [A bit harder] $G=Q_8$.

Solution:

Exercise 59. Given $m\geq1$ consider the 2×2 matrices

$$x=\begin{pmatrix} e^{\pi i/m} & 0\\ 0 & e^{-\pi i/m}\end{pmatrix} \text{ and } y=\begin{pmatrix} 0 & -1\\ 1 & 0\end{pmatrix}$$

Let $Q_{4m} = \langle x, y \rangle$ be the subgroup of $GL_2(\mathbb{C})$ that they generate. This is called the generalized quaternion group.

(i) Show that x is of order $2m$ and y is of order 4.

(ii) Show that $yxy^{-1} = x^{-1}$.

(iii) Deduce from Part (ii) that any element of Q_{4m} can be written in the form $x^i y^j$. Since $x^m = y^2$, we may assume $j = 0$ or 1. List the $4m$ elements of Q_{4m}.

(iv) Deduce from Part (ii) that for any l the subgroup $\langle x^l \rangle$ is normal in Q_{4m}.

(v) Show that if m is odd, Q_{4m} is a semidirect product of the normal subgroup $N = \langle x^2 \rangle$ by the subgroup $H = \langle y \rangle$, associated to the homomorphism $\phi\colon H \to \mathrm{Aut}(N) \cong U(\mathbb{Z}_m)$ given by $\phi(y) = \psi_{-1}$.

(vi) Conclude that Q_{12} as defined here is isomorphic to the group with that name in the lectures.

(vii) Show that Q_8 is not a semidirect product of proper subgroups.

Solution: