

## Groups and Symmetry — Exam solutions

- (1) (i)  $O_2$  is the group (under matrix multiplication) of all  $2 \times 2$  matrices  $A$  over  $\mathbb{R}$  for which  $A^T A = I$ .

The matrices  $R_\theta$  and  $S_\theta$  are given by

$$R_\theta = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

$$S_\theta = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix}$$

- (ii)

$$SO_2 = \{A \in O_2 \mid \det(A) = 1\}$$

$$C_n = \{1, R_{2\pi/n}, R_{4\pi/n}, \dots, R_{2(n-1)\pi/n}\}$$

$$D_n = \{1, R_{2\pi/n}, R_{4\pi/n}, \dots, R_{2(n-1)\pi/n}, S_0, S_{2\pi/n}, S_{4\pi/n}, \dots, S_{2(n-1)\pi/n}\}$$

- (iii) Let  $H$  be a finite subgroup of  $SO_2$ . Let  $\theta$  be the smallest angle in the range  $(0, 2\pi]$  such that  $R_\theta \in H$ . I claim that  $\theta = 2\pi/n$  for some  $n$ , and that  $H = C_n$ . To see this, let  $\phi$  be any angle such that  $\phi \geq 0$  and  $R_\phi \in H$ . 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  $R_\psi = R_\phi R_\theta^{-k} \in H$ . If  $\psi$  were in the range  $(0, 2\pi]$ , this would contradict our definition of  $\theta$ , so we must have  $\psi = 0$ . Thus  $\phi = k\theta$  and  $R_\phi = R_\theta^k$ . This shows that the elements of  $H$  are precisely the powers of  $R_\theta$ .

In particular, we have  $R_{2\pi} = I \in H$ , 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  $H$  consists of the powers of  $R_{2\pi/n}$ , in other words  $H = C_n$ .

- (iv) Suppose that  $K \leq O_2$  is a finite subgroup, and that  $K$  contains a reflection, say  $S_{2\theta} \in K$ . I claim that  $K = R_\theta D_n R_\theta^{-1}$  for some  $n$ . To see this, put  $K' = R_\theta^{-1} K R_\theta$ ; we need to show that  $K' = D_n$ . Clearly  $K'$  is a subgroup of  $O_2$ , containing the element  $R_\theta^{-1} S_{2\theta} R_\theta = S_0$ . Put  $H' = K' \cap SO_2$ ; by the previous part we have  $H' = C_n$  for some  $n$ . The group  $D_n$  is generated by  $C_n$  together with  $S_0$ , and both  $C_n$  and  $S_0$  are contained in  $K'$ , so  $D_n \leq K'$ . Conversely, suppose  $A \in K'$ . If  $\det(A) = +1$  then  $A \in K' \cap SO_2 = C_n$ , so  $A \in D_n$ . If  $\det(A) = -1$  then consider  $AS_0$ . This lies in  $K'$  (because both  $A$  and  $S_0$  do) and  $\det(AS_0) = +1$  so  $AS_0 \in K' \cap SO_2 = C_n$ , so  $A \in C_n \cdot S_0 \subseteq D_n$ . This shows that  $K' \subseteq D_n \subseteq K'$ , so  $K' = D_n$  as claimed.
- (v) If we rotate  $X$  clockwise through  $\pi/6$ , we obtain shape  $X'$  whose symmetry group is  $D_3$ . We thus have

$$H = \text{Symm}(R_{\pi/6} X') = R_{\pi/6} \text{Symm}(X') R_{\pi/6}^{-1} = R_{\pi/6} D_3 R_{\pi/6}^{-1}.$$

- (2) (i)  $\text{Isom}_2$  is the group of all functions  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  of the form  $f(x) = Ax + a$ , with  $A \in O_2$  and  $a \in \mathbb{R}^2$ . The function  $\psi: \text{Isom}_2 \rightarrow O_2$  is defined by  $\psi(f) = A$ , where  $f(x) = Ax + a$  as above.
- (ii) Consider two elements  $f$  and  $g$  of  $\text{Isom}_2$ , given by  $f(x) = Ax + a$  and  $g(x) = Bx + b$  say. Then

$$(f \circ g)(x) = f(g(x)) = A(Bx + b) + a = ABx + (Ab + b).$$

From this we see that  $\psi(f \circ g) = AB = \psi(f)\psi(g)$ , showing that  $\psi$  is a homomorphism.

- (iii) Let  $H$  be a subgroup of  $\text{Isom}_2$ . Then

$$\text{Trans}(H) = \{a \in \mathbb{R}^2 \mid T_a \in H\}$$

$$\psi(H) = \{A \in O_2 \mid A = \psi(h) \text{ for some } h \in H\}$$

- (iv)  $H$  is said to be a *wallpaper group* if (i)  $\psi(H)$  is finite, and (ii) there exist vectors  $u, v \in \mathbb{R}^2$ , linearly independent over  $\mathbb{R}$ , such that  $\text{Trans}(H) = \{nu + mv \mid n, m \in \mathbb{Z}\}$ .

- (v) Let  $H$  be a wallpaper group. Suppose that  $\psi(H) = C_n$ ; I claim that  $n \leq 6$ . If  $n = 1$  then there is nothing to prove, so we assume that  $n > 1$ . We can choose  $h \in H$  with  $\psi(h) = R_{2\pi/n}$ . Let  $w$  be a nonzero vector of minimal length in  $\text{Trans}(H)$ . Then  $T_w \in H$ , so  $hT_w h^{-1} \in H$ , but  $hT_w h^{-1} = T_{\psi(h)w} = T_{R_{2\pi/n}(w)}$ , so  $R_{2\pi/n}(w) \in \text{Trans}(H)$ . As  $\text{Trans}(H)$  is a subgroup of  $\mathbb{R}^2$ , it follows that the vector  $v = w - R_{2\pi/n}(w)$  also lies in  $\text{Trans}(H)$ . We know that  $\|v\| = 2 \sin(\pi/n)\|w\|$ , and this is nonzero because  $n > 1$ . As  $w$  has minimal length in  $\text{Trans}(H) \setminus \{0\}$ , we must therefore have  $2 \sin(\pi/n) \geq 1$ , so  $\sin(\pi/n) \geq 1/2 = \sin(\pi/6)$ , so  $n \leq 6$ .
- (3) (i) Let  $H$  be a subgroup of  $O_3$ , and suppose that  $-I \in H$ . Put  $G = H \cap SO_3$ , and define  $\phi: \{\pm 1\} \times G \rightarrow H$  by  $\phi(\epsilon, A) = \epsilon A$ . Then

$$\phi(\epsilon, A)\phi(\delta, B) = \epsilon A \delta B = \epsilon \delta AB = \phi(\epsilon \delta, AB),$$

showing that  $\phi$  is a homomorphism.

Now suppose that  $(\epsilon, A) \in \ker(\phi)$ , so  $\epsilon = \pm 1$  and  $A \in G$  and  $\epsilon A = I$ . We now take determinants, remembering that  $A \in G \leq SO_3$ , so  $\det(A) = 1$ ; we find that  $\epsilon^3 \det(A) = 1$  so  $\epsilon^3 = 1$  so  $\epsilon = 1$ . The equation  $\epsilon A = I$  now tells us that  $A = I$ , so  $(\epsilon, A) = (1, I)$ . This shows that the kernel of  $\phi$  is the trivial group, so  $\phi$  is injective. To prove that  $\phi$  is surjective, consider  $B \in H$ . Put  $\epsilon = \det(B)$  and  $A = \epsilon B$ . As  $B \in O_3$  we know that  $\epsilon = \pm 1$ , so  $\epsilon^2 = 1$ . It follows that  $\det(A) = \epsilon^3 \det(B) = \epsilon^4 = 1$ , so  $A \in SO_3$ . Moreover,  $\{I, -I\} \subseteq H$  so  $\epsilon I \in H$  so  $B = \epsilon A = (\epsilon I)A \in H$ . It therefore makes sense to consider  $\phi(\epsilon, B)$ , and we find that this is equal to  $\epsilon B = \epsilon^2 A = A$ . This proves that  $\phi$  is surjective as well as injective, so it is an isomorphism.

- (ii) (a) Let  $R_1$  be a half-turn around the  $x$ -axis, let  $R_2$  be a half-turn around the  $y$ -axis, and let  $R_3$  be a half-turn around the  $z$ -axis. This gives three distinct, nontrivial rotations in  $\text{Dir}(X)$ .
- (b) The formulae are

$$\begin{aligned} R_1(x, y, z) &= (x, -y, -z) \\ R_2(x, y, z) &= (-x, y, -z) \\ R_3(x, y, z) &= (-x, -y, z). \end{aligned}$$

(c) It follows that

$$R_1 R_2 R_3(x, y, z) = R_1 R_2(-x, -y, z) = R_1(x, -y, -z) = (x, y, z),$$

so  $R_1 R_2 R_3 = 1$ . We also have

$$\begin{aligned} R_1 R_2(x, y, z) &= (-x, -y, z) = R_2 R_1(x, y, z) \\ R_2 R_3(x, y, z) &= (x, -y, -z) = R_3 R_2(x, y, z) \\ R_3 R_1(x, y, z) &= (-x, y, -z) = R_1 R_3(x, y, z), \end{aligned}$$

showing that the matrices  $R_i$  commute with each other.

- (d) It is clear that the only lines of rotational symmetry for  $X$  are the  $x$ ,  $y$  and  $z$  axes, and thus that  $\text{Dir}(X) = \{1, R_1, R_2, R_3\}$ . We can identify  $C_2$  with  $\{1, -1\}$  and define  $\chi: \{\pm 1\} \times \{\pm 1\} \rightarrow SO_3$  by

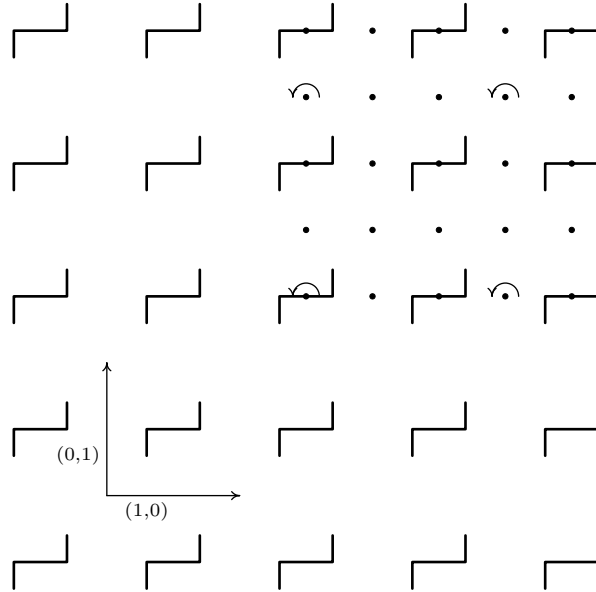
$$\chi(\epsilon, \delta) = \begin{pmatrix} \epsilon & 0 & 0 \\ 0 & \delta & 0 \\ 0 & 0 & \epsilon \delta \end{pmatrix}.$$

This is clearly a homomorphism, with

$$\begin{aligned} \chi(+1, +1) &= I & \chi(+1, -1) &= R_1 \\ \chi(-1, +1) &= R_2 & \chi(-1, -1) &= R_3. \end{aligned}$$

It follows that  $\chi$  gives an isomorphism  $C_2 \times C_2 \rightarrow G$ .

- (4) (i) There are no reflections or glide-reflections in  $G$  (because all the motifs point anti-clockwise, and any reflection or glide-reflection would make them point clockwise.) The translations in  $G$  are the maps  $T_{(n,m)}$  for  $n$  and  $m$  in  $\mathbb{Z}$ . There are rotations through  $\pi$  around all points of the form  $(n/2, m/2)$  with  $n, m \in \mathbb{Z}$ ; some of these centres are shown in the diagram below.



- (ii) Put  $T_1 = T_{(1,0)}$  and  $T_2 = T_{(0,1)}$ . I claim that  $T_1, T_2$  and  $R_\pi$  generate  $G$ . To see this, consider an element  $f_0 \in G$ . Clearly  $f_0$  must send the motif centred at  $(0,0)$  to the motif centred at  $(n, m)$  for some  $n$  and  $m$  in  $\mathbb{Z}$ . We put  $f_1 = T_1^{-n}T_2^{-m}f_0$ , so  $f_1 \in G$  and  $f_1(0,0) = (0,0)$ . This means that  $f_1$  is either a rotation about the origin, or a reflection across a line through the origin. As  $f_1$  must send the central motif to itself, we see that it must either be the identity or  $R_\pi$ . We also have  $f_0 = T_1^nT_2^mf_1$ , so either  $f_0 = T_1^nT_2^m$  or  $f_0 = T_1^nT_2^mR_\pi$ . Either way, we have expressed  $f_0$  in terms of  $T_1, T_2$  and  $R_\pi$ , showing that these isometries generate  $G$ .
- (iii)  $\text{Trans}(G)$  is just  $\mathbb{Z}^2$ , so the nonzero vectors of minimal length are  $(1,0), (-1,0), (0,1)$  and  $(0,-1)$ .
- (5) (i) Let  $G$  be a finite group, and  $p$  a prime. We can write  $|G| = p^v m$  where  $m$  is not divisible by  $p$ . A *Sylow  $p$ -subgroup* of  $G$  is a subgroup  $P \leq G$  such that  $|G| = p^v$ . We write  $n_p$  for the number of Sylow  $p$ -subgroups. The Sylow theorems state that
- There is at least one Sylow subgroup, so  $n_p > 0$ .
  - $n_p$  divides  $m$  and is congruent to 1 modulo  $p$ .
  - Any two Sylow  $p$ -subgroups are conjugate to each other.
- (ii) Let  $G$  be any group. The *centre* of  $G$  is the subgroup

$$ZG = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

- (iii) Let  $P$  be a group of order  $p^n$ , where  $p$  is prime and  $n > 0$ .
- (a) Suppose that  $P$  acts on a set  $X$ . Let the fixed points be  $x_1, \dots, x_r$ , so  $|\text{Fix}(X)| = r$ . The non-fixed points can be divided into orbits, say  $Y_1, \dots, Y_t$ . The order of  $Y_i$  divides  $|P| = p^n$ , so  $|Y_i| = p^{m_i}$  say. If  $Y_i$  was just a single point, then that point would form an orbit by itself, so it would be a fixed point. This is impossible because the  $Y_i$  are by definition the orbits of non-fixed points. This means that  $m_i > 0$ , so  $|Y_i| = p^{m_i} \equiv 0 \pmod{p}$ . It follows that

$$|X| = r + |Y_1| + \dots + |Y_t| \equiv r \pmod{p},$$

as claimed.

(b) Now let  $P$  act on itself by conjugation. We then have

$$\text{Fix}(P) = \{z \in P \mid gzg^{-1} = z \text{ for all } g \in G\} = ZG.$$

We thus have  $|ZG| = |\text{Fix}(P)| = |P| \pmod{p}$ , but also  $|P| = p^n = 0 \pmod{p}$ , so  $|ZG|$  is divisible by  $p$ , say  $|ZG| = pk$ . Moreover,  $1 \in ZG$  so  $ZG \neq \emptyset$ , so  $k > 0$ . This means that  $|ZG| \geq p$ , so  $ZG$  is nontrivial.

(iv) Let  $G$  be a group of order  $1225 = 5^2 \cdot 7^2$ .

(a) The Sylow theorems tell us that  $n_5$  divides 49 and is congruent to 1 modulo 5. The divisors of 49 are 1, 7 and 49, and these are congruent to 1, 2 and 4 modulo 5. Thus, the only possibility is  $n_5 = 1$ .

(b) Similarly, we know that  $n_7$  divides 25 (so  $n_7 \in \{1, 5, 25\}$ ) and  $n_7 \equiv 1 \pmod{7}$ . As  $5 \not\equiv 1 \pmod{7}$  and  $25 = 4 \not\equiv 1 \pmod{7}$  we see that the only possibility is  $n_7 = 1$ .

(c) Let  $P$  be the unique Sylow 5-subgroup, and let  $Q$  be the unique Sylow 7-subgroup, so  $|P| = 25$  and  $|Q| = 49$ . Note that uniqueness implies that  $P$  and  $Q$  are normal. Next, observe that the order of  $P \cap Q$  divides both  $|P| = 25$  and  $|Q| = 49$ , so  $|P \cap Q| = 1$ , so  $P \cap Q$  is the trivial group. I next claim that every element  $x \in P$  commutes with every element  $y \in Q$ . To see this, consider the commutator  $z = xy(yx)^{-1} = xyx^{-1}y^{-1}$ . We have  $x \in P$  and  $yx^{-1}y^{-1} \in yPy^{-1} = P$ , so  $z = x(yx^{-1}y^{-1}) \in P$ . We also have  $xyx^{-1} \in Q$  and  $y^{-1} \in Q$  so  $z = (xyx^{-1})y^{-1} \in Q$ . This means that  $z \in P \cap Q = \{1\}$ , so  $z = 1$ , so  $xy = yx$  as claimed.

We can now define  $\phi: P \times Q \rightarrow G$  by  $\phi(x, y) = xy$ . This is a homomorphism because  $P$  and  $Q$  commute. Let  $H$  be the image of  $\phi$ . This is a subgroup of  $G$ , which contains both  $P$  and  $Q$ . This means that  $|H|$  is a divisor of  $|G| = 5^2 7^2$ , and  $|H|$  is divisible by both  $|P| = 5^2$  and  $|Q| = 7^2$ . We must therefore have  $|H| = 5^2 7^2 = |G|$ , so  $H = G$ , proving that  $\phi$  is surjective. As  $|G| = |P \times Q|$ , it follows that  $\phi$  must actually be bijective, and thus an isomorphism.