Solutions to Sample Exam

1. Yes, S is a subgroup of G. The main property to verify is closure: If $x, y \in S$, then $f(xy) = f(x)f(y) = g(x)g(y) = g(xy)$, so $xy \in S$. Also note that S contains the identity element $1_G \in G$, since $f(1_G) = 1_H = g(1_G)$. Moreover, if $x \in S$ then $f(x^{-1}) = f(x)^{-1} = g(x)^{-1} = g(x^{-1})$, so $x^{-1} \in S$. So $S \leqslant G$.

2. Note that $T_\theta^{-1} = T_\theta$, $R_\alpha R_\beta = R_{\alpha+\beta}$ and $R_\theta^{-1} = R_{-\theta}$. For all θ, we have $T_\theta T_0 = R_{2\theta}$ as is seen either by considering the action of both sides on a pair of vectors (such as the unit vector on the positive x-axis, and a unit vector on the axis of T_θ) or using matrices:

$$T_\theta T_0 = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix} = R_{2\theta}\,.$$

In particular, $R_\theta = T_{\theta/2} T_0$ which gives (a). Also, solving for T_θ gives

$$T_\theta = R_{2\theta} T_0 = T_0 R_{-2\theta}\,.$$

Using these identities,

$$R_\theta T_\alpha R_\theta^{-1} = R_\theta (R_{2\alpha} T_0) R_{-\theta} = R_{\theta+2\alpha} T_0 R_{-\theta} = T_0 R_{-\theta-2\alpha} R_{-\theta} = T_0 R_{-2\theta-2\alpha} = T_{\alpha+\theta}\,.$$

So to solve (b), take $\theta = \beta - \alpha$.

All these solutions can be checked directly using 2×2 matrix representations for isometries.

3. Yes, θ is an automorphism of G. For all $A, B \in G$ we have

$$\theta(AB) = \tfrac{1}{\det(AB)} AB = \tfrac{1}{\det A}\tfrac{1}{\det B} AB = \left(\tfrac{1}{\det A} A\right)\left(\tfrac{1}{\det B} B\right) = \theta(A)\theta(B)$$

so $\theta : G \to G$ is a homomorphism. Moreover $\theta(\theta(A)) = A$ for all $A \in G$ so θ is its own inverse, i.e. $\theta^{-1} = \theta$ in $\operatorname{Aut} G$. But most importantly for our purposes, θ being invertible means that it is bijective.

4. We identify $S_5 < S_7$ as the subgroup consisting of all $\sigma \in S_7$ permuting $\{1, 2, 3, 4, 5\}$, while fixing both 6 and 7; that is, $\{\sigma \in S_7 : \sigma(6) = 6 \text{ and } \sigma(7) = 7\} = S_5$. Then H contains both S_5 and (67). By considering cycle structures, we see that in fact $H = \langle S_5, (67)\rangle$ which consists of all permutations of the form σ or $\sigma\cdot(67)$ where $\sigma \in S_5$. Thus $|H| = 2|S_5| = 240$ and in fact $H \cong S_5 \times C_2$ where $C_2 = \langle (67)\rangle$ is cyclic of order 2.

5. (a) Yes, G has a subgroup

$$\left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \,:\, a,b,c,d \in \mathbb{R},\ ad-bc \neq 0 \right\} \cong GL_2(\mathbb{R})$$

where the isomorphism is given by

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

(b) Yes; for example $\langle R_{2\pi/5} \rangle$ where the rotation by angle θ about the z-axis is given by

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

(c) Yes; for example consider the group of all rotations R_θ about the z-axis, as found in (b). Alternatively, consider all matrices of the form

$$\begin{pmatrix} 1 & b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad b \in \mathbb{R}.$$

6. Let's write $G = \{1, g, g^2, \ldots, g^{99}\} \cong C_{100}$ where $|g| = 100$. Recall *Euler's totient function* $\phi(n) = |\{i \in \{1,2,\ldots,n\} : \gcd(i,n) = 1\}|$, which is the number of generators (i.e. elements of order n) in a cyclic group of order n.

(a) For each d dividing 100, say $100 = dk$, G has $\phi(d)$ elements of order d. These elements are g^{ik} where $1 \leqslant i \leqslant d$ with $\gcd(i,d) = 1$. More explicitly, G has

1 element of order 1, namely 1;

1 element of order 2, namely g^{50};

2 elements of order 4, namely g^{25}, g^{75};

4 elements of order 5, namely $g^{20}, g^{40}, g^{60}, g^{80}$;

4 elements of order 10, namely $g^{10}, g^{30}, g^{70}, g^{90}$;

8 elements of order 20, namely g^{5i} for $i = 1,3,7,9,11,13,17,19$;

20 elements of order 25, namely g^{4i} for $i = 1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24$;

20 elements of order 50, namely g^{2i} for $i = 1,3,7,9,11,13,17,19,21,23,27,29,31,33,37,39,41,43,47,49$; and

40 elements of order 100, namely g^{10i+j} for $i \in \{0,1,2,3,4,5,6,7,8,9\}$ and $j \in \{1,3,7,9\}$.

(b) We discussed this in class. There are exactly 100 homomorphisms $\theta_k : G \to G$ defined by $\theta_k(x) = x^k$ for $x = 0,1,2,\ldots,99$. (In class I wrote $\phi_k(x) = x^k$ but

today I will try a different notation so as not to conflict with Euler's totient function ϕ. Greek letters are always popular for this. And I already used $\theta_k(x) = x^k$ in the T/F questions, so I'll go with that.)

(c) There are exactly $\phi(100) = 40$ automorphisms of C_{100}. (Here ϕ is Euler's totient function.) These are the maps θ_k for $\gcd(k, 100) = 1$. We have been doing examples like this ever since we started talking about endomorphisms and automorphisms of C_n, beginning with C_6.

(d) C_{100} has $\phi(100) = 40$ generators, i.e. elements of order 100, as listed in (a).

(e) (Finally, we have to think a little!) There are 80 such elements h, which are the elements of order 25, 50 or 100 listed above. This is because we need $\text{lcm}(|g|, |h|) = 100$, so $|h|$ must be divisible by 25.

7. (a) $G = A_6$ has $\binom{6}{4}3! = 90$ elements of order 4; these are the elements having the same cycle structure as $\sigma = (1\,2\,3\,4)(5\,6)$. They are all conjugate (they form a single conjugacy class of size 90).

(b) $G = A_6$ has $\binom{6}{5}4! = 144$ elements of order 5. These are partitioned into two conjugacy classes each of size 72, represented by $\sigma = (1\,2\,3\,4\,5)$ and $\sigma' = (1\,2\,3\,5\,4)$. (Any permutation in S_6 conjugating σ to σ' is necessarily an odd permutation.)

8. There are exactly four isomorphism types of *abelian* groups of order 100:

$$C_4 \times C_{25} \cong C_{100};$$
$$C_2 \times C_2 \times C_{25} \cong C_2 \times C_{50};$$
$$C_4 \times C_5 \times C_5 \cong C_5 \times C_{20}; \text{ and}$$
$$C_2 \times C_2 \times C_5 \times C_5 \cong C_{10} \times C_{10}.$$

9. We have $H = A_8$. Of course $H \subseteq A_8$ since all 7-cycles are even. Conversely, to show $A_8 \subseteq H$, it suffices to show that every product of two transpositions is contained in H, since these are generators of A_8. For example, $(12)(78) = (1876543)(1234567) \in H$. Applying an inner automorphism on both sides of this relation yields every 'double transposition' $(i, j)(k, \ell) \in H$ where i, j, k, ℓ are distinct. But if two transpositions $(i, j), (k, \ell)$ are not disjoint (so their product is a 3-cycle), it is easy to find another transposition (r, s) disjoint from both of them (so $r \neq s$ in $\{1, 2, \ldots, 8\}$ with $r, s \notin \{i, j, k, \ell\}$); and in this case we have shown that both $(i, j)(r, s) \in H$ and $(r, s)(k, \ell) \in H$, so we also have their product $(i, j)(k, \ell) \in H$.

10. Automorphisms of the given graph correspond to automorphisms of the 4-cycle with vertices 1,3,5,7, with the even-numbered vertices (2,4,6,8) coming along for the ride. So $G = \langle (1357)(2468), (28)(37)(46) \rangle \cong D_4$, a dihedral group of order 8. Simply

ignoring the even-numbered vertices gives an isomorphism $G \cong \langle (1357), (37) \rangle \cong D_4$, a dihedral group of order 8. (Whenever we identify a dihedral group of order 8 as a permutation group on the four vertices in this way, we are 'ignoring' the action on the other points of the square in exactly the same way, as these other points just get 'carried along for the ride'; they do not change the number of symmetries or the way their composition works.)

11. (a) T (b) T (c) T (d) F (e) F (f) F (g) F (h) F (i) T (j) F

Comments in #11:

(a) This is the statement of Cayley's Representation Theorem.

(b) Consider any nontrivial element $g \in G$ of order $n = |g| > 1$, and let p be a prime divisor of n; then $|g^{n/p}| = p$.

(c) Conjugation by y maps $xy \mapsto y(xy)y^{-1} = yx$.

(d) For example if $C_2 = \{1, g\}$, then the Klein four-group $C_2 \times C_2$ has a subgroup $\{(1,1), (g,g)\}$ which is not of the form $A \times B$.

(e) For example a Klein four-group $K = \{1, a, b, c\}$ has $\operatorname{Aut} K \cong S_3$ permuting a, b, c in all $3! = 6$ possible ways, and S_3 is nonabelian. More generally if V is the additive group of a vector space of dimension $\geqslant 2$, then $\operatorname{Aut} V$ contains invertible linear transformations which in general do not commute. (This is a well known property of invertible matrices.)

(f) In S_4, the elements (12) and (12)(34) of order 2 are not conjugate. Also, in a Klein four-group, no two of the elements of order 2 are conjugate. An even smaller counterexample is the two non-identity elements of order 3 in a cyclic group of order 3.

(g) Consider $\langle (12) \rangle \langle (13) \rangle = \{(), (12), (13), (132)\}$ in S_3.

(h) The easiest counterexample is $g = 1$ and $h \neq 1$ in any group of order at least 2. For a less trivial example, given a cyclic group $G = \{1, h, h^2, h^3\}$ of order 4, there is no homomorphism $\phi : G \to G$ satisfying $\phi(h^2) = h$, as this would require $\phi(1) = \phi(h^4) = h^2$.

(i) There exist integers r, s such that $rk + sn = 1$. Then $\theta_r(\theta_k(x)) = x^{rk} = x^{1-sn} = (x^n)^{-s}x = 1x = x$, so $\theta_r \circ \theta_k = \theta_k \circ \theta_r$ is the identity map $G \to G$. (Note: θ_k is not usually a homomorphism, unless G is abelian.)

(j) In class we gave an example of two nonisomorphic groups of order 27, both having 26 elements of order 3. See the solutions to HW2, #5(b), and compare with $C_3 \times C_3 \times C_3$.