Solutions for Problem Sheet 4

1. *Let $\varphi : G \to H$ be a group homomorphism, and let $g \in G$ be an element of finite order. Show that $\varphi(g)$ also has a finite order, in fact, $o(\varphi(g)) \mid o(g)$.*

Solution: Let $n = o(g)$. Then $(\varphi(g))^n = \varphi(g^n) = \varphi(1) = 1$, so $\varphi(g)$ has finite order, and $o(\varphi(g)) \mid n$.

2. *a) Suppose $G = \langle a \rangle \cong C_\infty$, and H is an arbitrary group. Prove that for every element h of H there exists exactly one homomorphism $\varphi : G \to H$ such that $\varphi(a) = h$.*

b) Prove that for a **finite** *group H, the only homomorphism $H \to C_\infty$ is the trivial homomorphism, that is, which maps every element to 1.*

Solution: a) The uniqueness follows from the fact that every element of $\langle a \rangle$ is of the form a^k for some $k \in \mathbb{Z}$, and for a homomorphism φ with $\varphi(a) = h$ we have $\varphi(a^k) = h^k$. Now we have to prove that $\varphi(a^k) = h^k$ ($k \in \mathbb{Z}$) gives a homomorphism. This map is well-defined since $o(a) = \infty$ implies that all $a^k \neq a^\ell$ if $k \neq \ell$. We only have to check that φ preserves the multiplication. Indeed, $\varphi(a^k a^\ell) = \varphi(a^{k+\ell}) = h^{k+\ell} = h^k h^\ell = \varphi(a^k)\varphi(a^\ell)$.

b) Suppose $C_\infty = \langle a \rangle$, so $\varphi(h) = a^k$ for some $k \in \mathbb{Z}$. Since $\langle h \rangle \leq H$ is finite, $o(h) = n$ for some positive integer n. But then $1 = \varphi(1) = \varphi(h^n) = a^{kn}$ implies $kn = 0$, so $k = 0$, thus $\varphi(h) = a^0 = 1$ for any $h \in H$.

3. *How many different homomorphisms exist between the two given groups?*

a) $C_{10} \to C_{33}$ *b)* $C_n \to C_n$ *c)* $C_n \to C_m$

Solution: a) Let $C_{10} = \langle a \rangle$ and $\varphi : C_{10} \to C_{33}$ be a homomorphism. Then $o(\varphi(a)) \mid o(a) = 10$, and $\langle \varphi(a) \rangle \leq C_{33}$ implies that $o(\varphi(a)) \mid 33$, which gives $o(\varphi(a)) \mid \gcd(10, 33) = 1$, so $\varphi(a) = 1$, and then $\varphi(a^k) = 1^k = 1$ for any other element $a^k \in C_{10}$. This shows that there is only one homomorphism, the trivial one, from C_{10} to C_{33}.

b),c) Note first that

(*) for a homomorphism $\varphi : C_n \to H$ the image $\operatorname{Im}\varphi \cong C_d$ for some $d \mid n$,

since for $C_n = \langle a \rangle$ the image $\operatorname{Im}\varphi = \{\, \varphi(x) \,|\, x \in \langle a \rangle \,\} = \{\, \varphi(a^k) \,|\, k \in \mathbb{Z} \,\} = \{\, \varphi(a)^k \,|\, k \in \mathbb{Z} \,\} = \langle \varphi(a) \rangle$ is a cyclic group, and $o(\varphi(a)) = d \mid o(a) = n$.

On the other hand, we can show that

(**) for $d \mid n$ there are exactly d different homomorphisms $\varphi : C_n \to C_d$.

Let $C_n = \langle a \rangle$ and $C_d = \langle b \rangle$. For any $k \in 0, 1, \ldots, d-1$ the map $\varphi(a^m) = b^{km}$ ($m \in \mathbb{Z}$) is well-defined: $a^m = a^\ell \Rightarrow a^{m-\ell} = 1 \Rightarrow d \mid n \mid m - \ell \Rightarrow d \mid k(m - \ell) \Rightarrow b^{k(m-\ell)} = 1 \Rightarrow b^{km} = b^{k\ell}$, and it clearly preserves the multiplication: $\varphi(a^{m+\ell}) = b^{k(m+\ell)} = b^{km}b^{k\ell} = \varphi(a^m)\varphi(a^\ell)$.

This shows that there are exactly n different homomorphisms $C_n \to C_n$, answering part b).

It also follows from (*) that in part c), the image of C_n is C_d for some divisor of n but $\operatorname{Im}\varphi \leq C_m$ also implies that $d \mid m$, so $d \mid \gcd(n, m)$. All these subgroups of C_m are included in the unique subgroup $C_{\gcd(n,m)}$ of C_m, so every homomorphism is actually a homomorphism $C_n \to C_{\gcd(n,m)}$, and their number is $\gcd(n, m)$ by (**).

4. *Let G be a group with $|G| = 91$. What is the number of homomorphisms $G \to G$ such that it maps at least two nonidentity elements of different order to 1?*

Solution: Suppose $\varphi : G \to G$ is a homomorphism, and $1 \neq a, b \in G$ have different orders such that $\varphi(a) = \varphi(b) = 1$. Note that the only divisors of $91 = 7 \cdot 13$ are $1, 7, 13, 91$, so $o(a), o(b) \in \{ 7, 13, 91 \}$.
If one of a and b has order 91 then this element generates the whole G, on the other hand, it is in $\operatorname{Ker}\varphi$, so $\operatorname{Ker}\varphi = G$, hence φ must be the trivial homomorphism, $\varphi = 1$.
In the remaining case $\{ o(a), o(b) \} = \{ 7, 13 \}$, and $a, b \in \operatorname{Ker}\varphi$, so $7, 13 \mid |\operatorname{Ker}\varphi| \Rightarrow 91 = \operatorname{lcm}(7, 13) \mid |\operatorname{Ker}\varphi \Rightarrow \operatorname{Ker}\varphi = G \Rightarrow \varphi = 1$.
Thus there is only one homomorphism $G \to G$, the trivial one.

5. *Let $G = \langle S \rangle$ and $H = \langle T \rangle$ for some $T \subseteq G$. Prove that $H \triangleleft G \Leftrightarrow t^s \in H$ for every $t \in T$ and $s \in S \cup S^{-1}$.*

Solution: It follows from the definition that if $H \triangleleft G$ then $t^s \in H$ for all $t \in T$ and $s \in S$. Conversely, suppose that $t^s \in H$ for any $t \in T$ and $s \in S \cup S^{-1}$, that is, $T^s = \{ t^s \mid t \in T \} \subseteq H$. The conjugation by s is a homomorphism, so for any $h = t_1^{\varepsilon_1} \cdots t_k^{\varepsilon_k} \in \langle T \rangle$ (where $t_i \in T$, $\varepsilon = \pm 1\ \forall i$), the conjugate by s is $h^s = (t_1^s)^{\varepsilon_1} \cdots (t_k^s)^{\varepsilon_k} \in H$, that is, $H^s \subseteq H$ for any $s \in S \cup S^{-1}$. But $x^{gh} = (gh)^{-1}x(gh) = h^{-1}g^{-1}xgh = h^{-1}x^g h = (x^g)^h$, and any $g \in G$ can be written as $g = s_1 \cdots s_m$ for some $s_i \in S \cup S^{-1}$, so $H^g = H^{s_1 \cdots s_m} = (H^{s_1})^{s_2 \cdots s_m} \subseteq H^{s_2 \cdots s_m} \subseteq \cdots \subseteq H^{s_m} \subseteq H$, thus $H \triangleleft G$.
Note that if every element of S has a finite order (in particular, if G is finite) then in the statement it is enought to take $s \in S$ because in this case s^{-1} is a positive power of s, so every element of G can be written as a product of elements of S.

6. *a) Show that in a group G, $ab = ba \Leftrightarrow a^b = a \Leftrightarrow b^a = b$.*
b) Show that the center $Z(G) = \{ z \in G \mid zg = gz\ \forall g \in G \}$ is a normal subgroup of G, in fact, any subgroup $H \leq Z(G)$ is a normal subgroup in G.

Solution: a) The equations $ab = ba$ and $b^{-1}ab = a$ can be transformed into each other by multiplication by b^{-1} (or back by b) from the left. Similarly, $ab = ba$ and $b = a^{-1}ba$ can be transformed into each other by multiplication by a^{-1}, and by a, respectively, from the left.

b) By part a), the definition of $Z(G)$ can also be written in the form: $Z(G) = \{ z \in G \mid z^g = z\ \forall g \in G \}$. The center is a subgroup: $1g = g1$ shows that $1 \in Z(G)$, then for $z, u \in Z(G)$ we have $(zu)^g = z^g u^g = zu$, so $zu \in Z(G)$, and $(z^{-1})^g = g^{-1}z^{-1}g = (g^{-1}zg)^{-1} = z^{-1}$ shows that $z^{-1} \in Z(G)$. Part a) also proves that $Z(G)$ is closed under conjugation, thus $Z(G) \triangleleft G$. In fact, if $H \leq Z(G)$ then for any $h \in H$ and $g \in G$, we have $h^g = h \in H$, so H is also a normal subgroup in G.

7. *a) Consider S_4 as the group of symmetries of the regular tetrahedron, acting on the four vertices. Show that the motions (orientation preserving isometries) of the tetrahedron form a normal subgroup in S_4. Which conjugacy classes of permutations are in this normal subgroup?*
b) Prove that the subset $\{ 1, (12)(34), (13)(24), (14)(23) \}$ is a normal subgroup in S_4.
c) There is an embedding φ of D_4 into S_4 mapping each isometry of the square 1234 to the corresponding permutation of the vertices. Prove that $\operatorname{Im}\varphi$ is not a normal subgroup of S_4.
d) Prove that S_4 has no other normal subgroups than 1, S_4 and the two subgroups defined in part a) and b).

Solution: a) The composition and inverses of orientation preserving isometries is also orientation preserving (and so is the identity map), so these isometries form a subgroup. We also proved that exactly half of all isometries of the regular tetrahedron are orientation preserving, so this subgroup has index 2, thus it must be a normal subgroup. If we consider the isometries as permutations of the four vertices, $1, 2, 3, 4$ then the rotations about axes going through one of the vertices are 3-cycles (...) on the other three vertices, and the $180°$ rotations about lines connecting the midpoints of opposite edges swap the endpoints of these edges, so we get the permutations with cycle structure (..)(..). Thus the twelve symmetries in this subgroup are all the permutations with cylce structures 1, (...) and (..)(..) (altogether $1 + 4 \cdot 2 + 3 = 12$).

b) This set (let it be called V) is clearly closed under conjugation: it is the union of two cojugacy classes, $\{ 1 \}$ and $\{(..)(..) \}$. We only have to prove that they form a subgroup. Since $x^2 = 1$ for all $x \in V$, it is closed for inverses, and also for products of the form 11, $1g$, $g1$ and gg, where $o(g) = 2$. If we take two different elements of order 2 in V, one is $(ab)(cd)$, and the other is $(ac)(bd)$ (we can write the elements in this order in the disjoint cycle decomposition), so their product is $(ab)(cd)(ac)(bd) = (ad)(bc)$ is the third element of order 2 in V.

c) The group D_4 has 2 elements of order 4 (these are (1234) and (4321)) but the conjugacy class of 4-cycles in S_4 consists of 6 elements, so this group cannot be closed for conjugation.

d) If $N \triangleleft S_4$ and $1 < |N|$ then N must be a union of at least two complete conjugacy classes of S_4, including $\{ 1 \}$. The sizes of the conjugacy classes of S_4 are: $| \{ 1 \} | = 1$, $| \{(..)(..) \} | = 3$, $| \{(..) \} | = 6$, $| \{(....) \} | = 6$ and $| \{(...) \} | = 8$. The Lagrange theorem implies that $|N| \mid |S_4| = 24$. The possible sums are $1 + 3$, $1 + 6$, $1 + 8$, $1 + 3 + 6$ $1 + 3 + 8$ or greater than 12 (in which case N should be S_4), and among these only $1 + 3 = 4$ and $1 + 3 + 8 = 12$ are divisors of 24. These two are exactly the normal subgroups defined in part b) and a).

8. *a) Determine the conjugacy classes, subgroups and normal subgroups of* D_4.

b) Embed D_4 *into* S_4 *by restricting the isometries on the set of the vertices* $\{ 1, 2, 3, 4 \}$ *of the square, and describe the elements of the image as permutations. Find two elements which are conjugate in* S_4 *but not conjugate in* D_4*, and give a conjugating permutation.*

Solution: a) Let r be the rotation by $90°$ and t one of the reflections. Then $\langle r \rangle \cap \langle t \rangle = 1$ implies that $| \langle t \rangle \langle r \rangle | = | \langle t \rangle | \cdot | \langle r \rangle |/1 = 2 \cdot 4 = 8$, so

$$D_4 = \{ r^k,\ tr^k \mid k = 0, 1, 2, 3 \} = \{ r^k,\ tr^k \mid k = 0, 1, 2, -1 \}$$

where r^k are the rotations and tr^k the reflections. We can also notice that if we apply a reflection, then a rotation, and then the same reflection again then we get a rotation by the same degree in the opposite direction:

$$trt = r^{-1}, \text{ or equivalently, } t^{-1}rt = r^{-1},$$

since $o(t) = 2$. So the conjugate of a rotation by a reflection is the inverse of the rotation. Note also that, since every element of D_4 can be written as a product of t's and r's, a subset is closed under conjugation in D_4 if and only if it is closed under conjugation by t and r. From the equation $t^{-1}rt = r^{-1}$, we can quickly deduce that

$$r^{-1}tr = tt^{-1}r^{-1}tr = t(t^{-1}rt)^{-1}r = t(r^{-1})^{-1}r = tr^2, \text{ and}$$
$$r^k t = tt^{-1}r^k t = t(t^{-1}rt)^k = tr^{-k},$$

and using these, we can calculate the conjugates of the elements of D_4 by t and r.

g	1	r	r^2	r^{-1}	t	tr	tr^2	tr^{-1}
$t^{-1}gt$	1	r^{-1}	r^2	r	t	tr^{-1}	tr^2	tr
$r^{-1}gr$	1	r	r^2	r^{-1}	tr^2	tr^{-1}	t	tr

This shows that the conjugacy classes are

$$\{1\}, \quad \{r^2\}, \quad \{r, r^{-1}\}, \quad \{t, tr^2\}, \quad \{tr, tr^{-1}\}.$$

The one-element conjugacy classes contain the elements of the center of the group, that is, those elements whose conjugates by any element are themselves, so $Z(G) = \{1, r^2\}$. Every normal subgroup is the union of some conjugacy classes. The nontrivial conjugacy classes generate a subgroup which contains r^2 (for the two-element conjugacy classes $\{a, b\}$, $a^{-1}b = r^2$), so $\langle r^2 \rangle$ is part of the nontrivial normal subgroups. $\langle r^2 \rangle = Z(G)$ is a normal subgroup, and besides this, 1 and G, there are only 4-element normal subgroups by the Lagrange theorem, that is, the union of $\{1, r^2\}$ and one of the two-element conjugacy classes. These all form subgroups: $\{1, r^2, r, r^{-1}\} = \langle r \rangle \cong C_4$, and the other two, $\{1, r^2, t, tr^2\}$ and $\{1, r^2, tr, tr^{-1}\}$ contain only elements of order 1 or 2, and it is easy to check that the product of any two nontrivial elements gives the third, thus these are also normal subgroups, and they are isomorphic to the Klein group.

By the Lagrange Theorem, the subgroups of G, apart from 1 and G can only be of order 2 or 4, and those of order 4 have index 2, so they must be normal. We have already listed them. What remains are the subgroups of order 2. But groups of prime order are cyclic, so the subgroups of order 2 are generated by elements of order 2. They are $\langle t \rangle, \langle tr \rangle, \langle tr^2 \rangle, \langle tr^{-1} \rangle, \langle r^2 \rangle$.

b) It $\tau = (12)(34)$ and $\rho = (1234)$ are the permutations corresponding to the isometries t and r, respectively, then the conjugacy classes are $\{1\}$, $\{\rho^2\} = \{(13)(24)\}$, $\{\rho, \rho^{-1}\} = \{(1234), (1432)\}$, $\{\tau, \tau\rho^2\} = \{(12)(34), (14)(23)\}$ and $\{\tau\rho, \tau\rho^{-1}\} = \{(13), (24)\}$. $\rho^2 = (13)(24)$ and $\tau = (12)(34)$ are not conjugate in $\langle \tau, \rho \rangle \cong D_4$, but they are conjugate in S_4, since they have the same cycle structure. We can find a conjugating element if we write the second permutations under the first (adjusting the order of the cycles if necessary), and map every element to the one below it:

$$\begin{matrix}(13)(24)\\(12)(34)\end{matrix} \text{ gives } g = (23) \in S_4$$

so $(\rho^2)^g = \tau$.

HW1. *Let $x = (1345)(27)$ and $y = (28)(3156)$ be elements of the symmetric group S_8. Calculate the expressions xy and $x^y = y^{-1}xy$, and find a permutation $h \in S_8$ such that $x^h = y$.*

HW2. *Suppose that the subgroups $A, B \leq G$ are commutative, and $AB = G$. Prove that $A \cap B \lhd G$.*