Solutions for the Practice Questions for the Final

A. Let σ be the following element in S_9:

$$\sigma \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 2 & 4 & 8 & 7 & 9 & 1 & 6 \end{pmatrix} \quad .$$

(a) Find the cycle decomposition of σ.

Solution. Here are the orbits:

$$1 \mapsto 3 \mapsto 2 \mapsto 5 \mapsto 8 \mapsto 1, \qquad 4 \mapsto 4, \qquad 6 \mapsto 7 \mapsto 9 \mapsto 6$$

and so we have the following cycle decomposition for σ:

$$\sigma \;=\; (1\ 3\ 2\ 5\ 8)(4)(6\ 7\ 9) \;=\; (1\ 3\ 2\ 5\ 8)(6\ 7\ 9) \quad .$$

(b) Does there exist an element $\tau \in S_9$ such that $\tau\sigma\tau^{-1} = \sigma^4$? If so, find such a τ. If not, explain why.

Solution. Since (1 3 2 5 8) and (6 7 9) and have orders 5 and 3, respectively, we have

$$(1\ 3\ 2\ 5\ 8)^4 \;=\; (1\ 3\ 2\ 5\ 8)^{-1} \;=\; (8\ 5\ 2\ 3\ 1) \qquad \textit{and} \qquad (6\ 7\ 9)^4 \;=\; (6\ 7\ 9) \quad .$$

Since (1 3 2 5 8) and (6 7 9) are disjoint cycles, they commute with each other. Therefore,

$$\sigma^4 \;=\; \big((1\ 3\ 2\ 5\ 8)(6\ 7\ 9)\big)^4 \;=\; (1\ 3\ 2\ 5\ 8)^4(6\ 7\ 9)^4 \;=\; (8\ 5\ 2\ 3\ 1)(6\ 7\ 9) \quad ,$$

which is a product of disjoint cycles of lengths 5 and 3, just like σ. As discussed in class, σ and σ^4 must therefore be conjugate in S_9. By the Conjugacy Principle, we can take

$$\tau \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 5 & 4 & 3 & 6 & 7 & 1 & 9 \end{pmatrix} \quad .$$

With this choice of τ, we have $\tau\sigma\tau^{-1} = \sigma^4$.

(c) Does there exist an element $\tau \in S_9$ such that $\tau\sigma\tau^{-1} = \sigma^6$? If so, find such a τ. If not, explain why.

Solution. Note that $|\sigma| = 15$. Note also that $gcd(6, 15) = 3$. Therefore, we have a formula

$$\left|\sigma^6\right| \;=\; \frac{15}{3} \;=\; 5$$

Since the orders of σ and σ^6 are not equal, those elements of S_9 cannot be conjugate in S_9. Therefore, no such τ exists.

B. Consider the element $\sigma = (1\ 3)(2\ 4)$ in S_4. Let $C(\sigma)$ denote the centralizer of σ in S_4. Determine $C(\sigma)$. (Hint: Proposition 5 on the handout about Conjugacy might be helpful.)

Solution. Note that there are exactly three elements in S_4 with the same cycle decomposition type as σ. Thus, the conjugacy class of σ has cardinality equal to 3. Therefore, by proposition 5 on the conjugacy handout, we have $[S_4 : C(\sigma)] = 3$. Thus $|S_4|/|C(\sigma)| = 3$. It follows that $\left|C(\sigma)\right| = 8$.

Note that $\sigma \in D_4$. In fact, σ corresponds to a 180^o rotation of the square. We know that the center $Z(D_4) = \{e,\ \sigma\}$. Thus, σ commutes with every element of D_4. It follows that $D_4 \subseteq C(\sigma)$. Both of those groups have order 8. Therefore, we must have $D_4 = C(\sigma)$. This determines $C(\sigma)$. We have $C(\sigma) = D_4$.

C. Suppose that G is a group. Suppose that N is a normal subgroup of G and that $|N| = 2$. Prove that $N \subseteq Z(G)$.

Solution Since N has order 2, we have $N = \{e,\ n\}$, where e is the identity element in G and $n \neq e$. Thus, n has order 2. If $g \in G$, then gng^{-1} also has order 2. Since N is a normal subgroup of G, we know that $gng^{-1} \in N$ for all $g \in G$. The only element in N of order 2 is n itself. Hence we must have $gng^{-1} = n$ for all $g \in G$. That is, $gn = ng$ for all $g \in G$. It follows that $n \in Z(G)$. Of course, we also have $e \in Z(G)$. Therefore, $N \subseteq Z(G)$, as stated. We have proved that N is a subgroup of $Z(G)$.

D. Suppose that G is a group and that M and N are normal subgroups of G. Assume also that $M \cap N = \{e\}$, where e is the identity element in G. Suppose that $m \in M$ and $n \in N$. Prove that $mn = nm$.

Solution. We will assume that $m \in M$ and $n \in N$. We want to prove that $mn = nm$. Equivalently, we want to prove that $(mn)(nm)^{-1} = e$, where e is the identity element of G. Let

$$g \;=\; (mn)(nm)^{-1} \;=\; mnm^{-1}n^{-1} \quad .$$

We want to prove that $g = e$. Note that

$$g \;=\; \big(mnm^{-1}\big)n^{-1} \qquad \textit{and} \qquad g \;=\; m\big(nm^{-1}n^{-1}\big) \;\;.$$

Since N is a normal subgroup of G and $m \in G$, we have $mNm^{-1} \subseteq N$. Thus, $mnm^{-1} \in N$. Since $n^{-1} \in N$, we have

$$g \;=\; \big(mnm^{-1}\big)n^{-1} \;\in\; N \;\;.$$

Since M is a normal subgroup of G and $n \in G$, we have $nMn^{-1} \subseteq N$. Since $m^{-1} \in M$, it follows that $nm^{-1}n^{-1} \in M$. Since $m \in M$, we then have

$$g \;=\; m\big(nm^{-1}n^{-1}\big) \;\in\; M \;\;.$$

We have proved that $g \in N$ and that $g \in M$. It follows that $g \in M \cap N$. Since we are assuming that $M \cap N = \{e\}$, it follows that $g = e$. As pointed out above, it follows that $mn = nm$, which is what we wanted to prove.

E. Let $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For each of the following groups G, determine if G has a subgroup isomorphic to A. Justify your answers fully.

$$G = S_3, \qquad G = S_4 \;\;, \qquad G = Q_8 \;\;,$$

$$G = D_4 \;\;, \qquad G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \;\;, \qquad G = \mathbb{Z}/48\mathbb{Z} \;\;.$$

Solution. The group $G = S_3$ has no subgroup isomorphic to A. Justification: Since $|G| = 6$, any subgroup of G has order dividing 6. Hence G cannot have a subgroup of order 4. But $|A| = 4$ and any group isomorphic to A must have order 4.

The group $G = S_4$ has a subgroup isomorphic to A, namely the Klein 4-group

$$V \;=\; \{\; e,\; (1\;2)(3\;4),\; (1\;3)(2\;4),\; (1\;4)(2\;3)\;\}$$

We know that V is a subgroup of S_4. If we let $H = \langle (1\;2)(3\;4) \rangle$ and $K = \langle (1\;3)(2\;4) \rangle$. Then H and K are subgroups of V of order 2 and we have $H \cap K = \{e\}$. Furthermore, since V is abelian, every element of H commutes with every element of K. Also, it is clear that $HK = V$. As proved in class one day, it follows that $V \cong H \times K$. Both H and K are cyclic of order 2. Therefore, both H and K are isomorphic to $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$. It follows that $V \cong A$.

The quaternionic group $G = Q_8$ has no subgroup isomorphic to A. In fact, G has only one element of order 2, namely -1. Therefore, if H is any subgroup of G of order 4, then H must contain an element of order 4. Thus, H cannot be isomorphic to A because A has no elements of order 4.

The group $G = D_4$ has a subgroup isomorphic to A. Using the definition given in class, we can regard D_4 as a subgroup of S_4. That subgroup contains the Klein 4-group V. As pointed out above, V is isomorphic to A. Hence D_4 contains a subgroup isomorphic to A.

The group $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ contains a subgroup isomorphic to A. We will use additive notation for G. Since G is abelian, the map $\phi : G \to G$ defined by $\phi(g) = 2g$ for all $g \in G$ is a homomorphism. Let

$$K \;=\; Ker(\phi) \;=\; \{\; g \in G \mid 2g = e \;\}$$

where e is the identity element of G. Of course, K is a subgroup of G. Using the standard notation for congruence classes, this subgroup H is as follows:

$$K \;=\; \{\; \big([0]_4,\; [0]_2\big),\; \big([0]_4,\; [1]_2\big),\; \big([2]_4,\; [0]_2\big),\; \big([2]_4,\; [1]_2\big) \;\}$$

It is clear that K is isomorphic to the direct product of two cyclic groups of order 2, and hence K is isomorphic to A.

The group $G = \mathbb{Z}/48\mathbb{Z}$ has no subgroup isomorphic to A. Justification: Since G is cyclic, every subgroup of G must also be cyclic. But A is not cyclic. Any group isomorphic to A will also fail to be cyclic. Hence no subgroup of G can be isomorphic to A.

F: Recall that $\mathbb{R}$ is a group under $+$ and that $\mathbb{Z}$ is a subgroup of $\mathbb{R}$.

(a) Explain why $\mathbb{Z}$ is a normal subgroup of $\mathbb{R}$.

Solution. The group $\mathbb{R}$ under the operation $+$ is abelian. Hence every subgroup of $\mathbb{R}$ is normal. Obviously, $\mathbb{Z}$ is a subgroup of $\mathbb{R}$ and hence must be a normal subgroup of $\mathbb{R}$.

(b) Show that $\mathbb{R}/\mathbb{Z}$ contains infinitely many elements of finite order.

Solution. The elements of $\mathbb{R}/\mathbb{Z}$ are of the form $r + \mathbb{Z}$, where $r \in \mathbb{R}$. The elements of $\mathbb{Q}/\mathbb{Z}$ are of the form $a + \mathbb{Z}$, where $a \in \mathbb{Q}$. We can regard $\mathbb{Q}/\mathbb{Z}$ as a subgroup of $\mathbb{R}/\mathbb{Z}$. Every element of $\mathbb{Q}/\mathbb{Z}$ has a finite order (a fact proved in one of the homework problems). Also,

$\mathbb{Q}/\mathbb{Z}$ is an infinite group. Thus, the infinite subgroup $\mathbb{Q}/\mathbb{Z}$ of $\mathbb{R}/\mathbb{Z}$ consists of elements of finite order.

(c) How many elements in $\mathbb{R}/\mathbb{Z}$ have order 7? How many elements have order 49?

Solution.. Consider $r+\mathbb{Z}$, where $r \in \mathbb{R}$. The identity element in $\mathbb{R}/\mathbb{Z}$ is $0+\mathbb{Z} = \mathbb{Z}$. Also,

$$7(r+\mathbb{Z}) = 0+\mathbb{Z} \iff 7r \in \mathbb{Z} \iff r = \frac{m}{7} \text{ with } m \in \mathbb{Z} \ .$$

Also, if m is not divisible by 7, then $r \notin \mathbb{Z}$, and $r+\mathbb{Z} \neq \mathbb{Z}$. It follows that if r has denominator equal to 7, then $r+\mathbb{Z}$ has order 7. All the element of $\mathbb{R}/\mathbb{Z}$ of order 7 are of that form. An example of an element of order 7 in $\mathbb{R}/\mathbb{Z}$ is $g = \frac{1}{7}+\mathbb{Z}$. All the element of $\mathbb{R}/\mathbb{Z}$ of order 7 (which we just described) are of the form mg, where $m \in \mathbb{Z}$. Thus, they are in the cyclic subgroup $\langle g \rangle$ which has order 7. There are six elements in that subgroup, apart from the identity element. They are the elements of order 7 in $\mathbb{R}/\mathbb{Z}$. Thus, $\mathbb{R}/\mathbb{Z}$ has exactly six elements of order 7.

For similar reasons to the above, any element of order 49 in $\mathbb{R}/\mathbb{Z}$ will be of the form $r+\mathbb{Z}$, where $r = \frac{m}{49}+\mathbb{Z}$, where $gcd(m,\ 49) = 1$. They are all in the cyclic subgroup of $\mathbb{R}/\mathbb{Z}$ generated by $g = \frac{1}{49}+\mathbb{Z}$. Thus, we must just determine the number of elements of order 49 in a cyclic group of order 49. The elements in a cyclic group of order 49 have orders 1, 7, and 49. Exactly one element has order 1, exactly six elements have order 7. Therefore the number of elements of order 49 in $\mathbb{R}/\mathbb{Z}$ is 49-7=42.

(d) Show that $\mathbb{R}/\mathbb{Z}$ contains infinitely many elements of infinite order.

Solution. One element of infinite order is $g = \sqrt{2}+\mathbb{Z}$. To verify this, assume to the contrary that g has finite order. Then, for some positive integer m, we would have $mg = \mathbb{Z}$. That is, we would have $m\big(\sqrt{2}+\mathbb{Z}\big) = \mathbb{Z}$. Equivalently, $m\sqrt{2}+\mathbb{Z} = \mathbb{Z}$. This would mean that $m\sqrt{2} \in \mathbb{Z}$. It would follow that $m\sqrt{2} = n$, where $n \in \mathbb{Z}$, and hence $\sqrt{2} = n/m$. This contradicts the fact that $\sqrt{2}$ is irrational.

Since $g = \sqrt{2}+\mathbb{Z}$ has infinite order, the subgroup $\langle g \rangle$ of $\mathbb{R}/\mathbb{Z}$ is an infinite cyclic group and hence is isomorphic to $\mathbb{Z}$, considered as a group under addition. Every nonzero element of $\mathbb{Z}$ has infinite order. Therefore, every element of $\langle g \rangle$, except for the identity element, must have infinite order.

G. In this problem, suppose that G and G' are groups and that $\varphi : G \to G'$ is a homomorphism. Suppose that $a \in G$ and that $|a| = m$, where $m \geq 1$.

(a) Prove that $|\varphi(a)|$ divides m.

Solution.. Since $|a| = m$, we have $a^m = e$, the identity element in G. Since φ is a homomorphism, we know that $\varphi(e) = e'$, the identity element in G'. We also have $\varphi(a^m) = \varphi(a)^m$. Therefore,

$$\varphi(a)^m \;=\; \varphi(a^m) \;=\; \varphi(e) \;=\; e' \quad .$$

Since $\varphi(a)^m = e'$, it follows that the order of $\varphi(a)$ divides m. That is, $|\varphi(a)|$ divides m.

(b) Let $N = Ker(\varphi)$. Suppose that N is finite and that $gcd(m,\ |N|) = 1$. Prove that $|\varphi(a)| = m$.

Solution. Let $n = |\varphi(a)|$. From part (a), we know that n divides m. Let $d = m/n$. Then d is a positive integer and $m = nd$. Furthermore,

$$\varphi(a^n) \;=\; \varphi(a)^n \;=\; e' \quad .$$

Therefore, $a^n \in Ker(\varphi)$. That is, $a^n \in N$. Notice that $(a^n)^d = a^m = e$. Thus, a^n is an element of N and $|a^n|$ must divide d. But, N is assumed to be a finite group and we know that the order of every element of N must divide $|N|$. Thus, $|a^n|$ must divide $|N|$ and must also divide d. Since d divides m, it follows that $|a^n|$ must divide both $|N|$ and m.

We are assuming that $gcd(m,\ |N|) = 1$. Since $|a^n|$ is a common divisor of m and $|N|$, it follows that $|a^n| = 1$. Therefore, $a^n = e$. Thus, $m = |a|$ must divide n. But $m = nd$ and so n also divides m. Therefore, $n = m$. That is, $|\varphi(a)| = m$, which is what we wanted to prove.

(c) Give a specific example where $|a| = 25$ and $|\varphi(a)| = 5$. Justify your answer. (Note: You must specify G, G', φ, and a in your example.)

Solution. Let G be a cyclic group of order 25. Let a be a generator of G. Then $|a| = 25$. Let $G' = G$. Consider the map $\varphi : G \to G$ defined by $\varphi(g) = g^5$ for all $g \in G$. Notice that φ is a homomorphism of G to G. To see this, note that if $x, y \in G$, then

$$\varphi(xy) \;=\; (xy)^5 \;=\; x^5y^5 \;=\; \varphi(x)\varphi(y) \quad .$$

Now $\varphi(a) = a^5$. We know that $|a^5| = \frac{25}{gcd(5,25)} \;=\; \frac{25}{5} = 5$. Here we are using proposition 8 on the handout about cyclic groups and orders of elements. It follows that $|\varphi(a)| = 5$ and $|a| = 25$, as we wanted.

To give a specific example, we take $G = G' = \mathbb{Z}_{25}$ and $a = 1 + 25\mathbb{Z}$. Note that the group operation is $+$. Thus, we define φ by $\varphi(g) = 5g$ for all $g \in G$.