Solutions for the practice questions for the midterm

1. Suppose that G is an abelian group and that $a,\ b \in G$. Suppose that $|a| = 3$ and $|b| = 5$. Prove that $|ab| = 15$.

Solution. Let e be the identity element in G. Let $k \in \mathbf{Z}$. Since $|a| = 3$, it follows that $a^k = e$ if and only if 3 divides k. Also, since $|b| = 5$, it follows that $b^k = e$ if and only if 5 divides k. In particular, we have $a^{15} = e$ and $b^{15} = e$. Since G is abelian, we have

$$(ab)^{15} \ = \ a^{15}b^{15} \ = \ ee \ = e$$

Since $(ab)^{15} = e$, it follows that $|ab|$ divides 15. That is, we have

$$|ab| \ \in \ \{ \ 1, \ 3, \ 5, \ 15 \ \} \quad .$$

However, notice that

$$(ab)^3 \ = \ a^3b^3 \ = \ eb^3 \ = \ b^3 \ \neq \ e, \qquad \textit{and} \qquad (ab)^5 \ = \ a^5b^5 \ = \ a^5e \ = \ a^5 \ \neq \ e \ \ ,$$

the reason being that 5 does not divide 3 and 3 does not divide 5, respectively. It follows that $|ab|$ does not divide 3 and that $|ab|$ does not divide 5. This leaves just one possibility. Namely, it follows that $|ab| = 15$, which is the statement we wanted to prove.

2. Suppose that G is a group and that $c \in G$. Suppose that $|c| = 15$. Prove that there exist elements $a,\ b \in G$ such that $|a| = 3,\ \ |b| = 5$, and $ab = c$.

Solution. Let $H = \langle c \rangle$, the cyclic subgroup of G generated by c. We will find elements $a,\ b \in H$ with the desired properties. Notices that

$$\langle c^5 \rangle \ = \ \{ \ e, \ c^5, \ c^{10} \ \} \qquad \textit{and} \qquad \langle c^3 \rangle \ = \ \{ \ e, \ c^3, \ c^6, \ c^9, \ c^{12} \ \},$$

and that all the elements in the first group (except for e) have order 3, and that all the elements in the second group (except for e) have order 5. Furthermore, notice that

$$c \ = \ c^{16} \ = \ c^{10}c^6 \quad .$$

We can choose $a = c^{10}$ and $b = c^6$. Then $a, b \in G$, and $|a| = 3,\ |b| = 5$, and $ab = c$, as we wanted.

3. Let $G = S_8$. Show that there exist elements $a,\ b \in G$ such that $|a| = 3$ and $|b| = 5$, but $|ab| \neq 15$.

Solution. We pick $a = (1\ \ 2\ \ 3)$ and $b = (1\ \ 2\ \ 3\ \ 4\ \ 5)$, considered as elements of S_8. Then

$$c \ = \ ab \ = \ (1\ \ 3\ \ 4\ \ 5\ \ 2)$$

In fact, we have $|a| = 3$ and $|b| = 5$, but $|ab| = 5 \neq 15$.

It is worth remarking that S_8 contains the following subgroup

$$H = \ \{ \ \sigma \in S_8 \ \big| \ \sigma(6) = 6, \ \sigma(7) = 7, \ \textit{and} \ \sigma(8) = 8 \ \}$$

which is isomorphic to S_5. We decided to choose $a, b \in H$. Hence $ab \in H$ too. But S_5 has no elements of order 15. (Consider the possible cycle decomposition types for elements in S_5.) Since $H \cong S_5$, it follows that H also has no elements of order 15. Therefore, ab could not possibly have order 15.

4. Let σ be the following element in S_9:

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

(a) Find the cycle decomposition of σ.

Solution. We notice the following orbits under the action of powers of σ:

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

and hence the cycle decomposition of σ is

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

(b) Let $H = \langle \sigma \rangle$, the cyclic subgroup of S_9 generated by σ. Determine $|H|$.

Solution. We know that $|H| = |\sigma|$. The cycle decomposition for σ tells us that the order of σ is the least common multiple of the cycle lengths 5 and 4. Thus, $|\sigma| = lcm(5, \ 4) = 20$. Therefore, $|H| = 20$.

(c) Does there exist an element $\tau \in S_9$ such that $\tau\sigma\tau^{-1} = \tau^3$? If so, find such a τ. If not, explain why.

Solution. Multiplying the stated equation by τ^{-1} on the left and by τ on the right, we obtain the equation $\sigma = \tau^3$. The group H is a cyclic group of order 20. Suppose that r is an integer such that $gcd(r, 20) = 1$. As explained in class, the map $\varphi : H \to H$ defined by $\varphi(h) = h^r$ is an automorphism of H. In particular, φ is a bijection of H to itself. Take $r = 3$. Obviously, $gcd(3, 20) = 1$. Thus, there must exist an element $\tau \in H$ such that $\varphi(\tau) = \sigma$. This means that $\tau^3 = \sigma$. Since H is a subgroup of S_9, we have $\tau \in S_9$.

Alternatively, and explicitly, we can simply notice that $\tau = \sigma^7$ works. Indeed, for that choice of τ, we have

$$\sigma \ = \ \sigma^{21} \ = \ (\sigma^7)^3 \ = \ \tau^3 \ .$$

(d) Does there exist an element $\tau \in S_9$ such that $\tau\sigma\tau^{-1} = \tau^2$? If so, find such a τ. If not, explain why.

Solution. As in part (c), the stated equation is equivalent to $\sigma = \tau^2$. If such a $\tau \in S_9$ exists, then we claim that $|\tau| = 40$. To see this, let $m = |\tau|$. It is clear that

$$\tau^{40} \ = \ (\tau^2)^{20} \ = \ \sigma^{20} \ = \ e$$

and hence m divides 40. However,

$$\sigma^m \ = \ \tau^{2m} \ = \ (\tau^m)^2 \ = \ e^2 \ = \ e \ .$$

Since $|\sigma| = 20$, it follows that m is divisible by 20. It follows that $m \in \{20, \ 40\}$. On the other hand,

$$\tau^{20} \ = \ (\tau^2)^{10} \ = \ \sigma^{10} \ \neq \ e$$

since $10 < 20$ and $|\sigma| = 20$. Thus, $m \neq 20$. Therefore, $m = 40$, as claimed.

Thus, $\tau \in S_9$ and $|\tau| = 40$. But no such τ exists. To verify that, consider the cycle decomposition of τ. There are many possibilities. The length of each k-cycle in the cycle decomposition of τ must divide 40 and the sum of the lengths is 9. If there is no 8-cycle in that decomposition, then the lengths will not be divisible by 8. The lcm of the lengths will not be divisible by 8 and cannot equal 40. However, if there is a cycle of length 8, then τ is a product of an 8-cycle and a 1-cycle, and will have order 8 instead of order 40. We have proved that S_9 has no elements of order 40. It follows that the equation $\sigma = \tau^2$ cannot hold for any $\tau \in S_9$.

5. Give an example of a nonabelian group G of order 42.

Solution. Suppose that $G = A \times B$, where A and B are groups. It is clear that G is abelian if and only if both A and B are abelian. Also, we know that $|G| = |A||B|$ if A and B are finite groups. For this problem, let $A = S_3$ and $B = \mathbb{Z}_7$. Thus, if we take $G = A \times B$, then $|G| = 6 \cdot 7 = 42$. Also, since A is nonabelian, G must be nonabelian too.

6. Give two examples of non-isomorphic groups G such that G is nonabelian, but every proper subgroup of G is cyclic.

Solution. One example is S_3. It is a nonabelian group. Another example is the quaternion group Q_8 of order 8. By inspection, one can determine all the subgroups. The proper subgroups of S_3 are cyclic of orders 1, 2 or 3. The proper subgroups of Q_8 are cyclic of orders 1, 2, or 4.

7. Give an example of a group G such that G is nonabelian, every proper subgroup of G is abelian, and at least one proper subgroup is not cyclic.

Solution. One example is D_4, a group of order 8. The proper subgroups have order 1, 2, or 4 and must be abelian. (We proved in class that any finite group of order ≤ 5 must be abelian.). However, D_4 has a subgroup of order 4 in which every element has order 1 or 2. To describe such a subgroup, let us number the vertices of a square clockwise by 1, 2, 3, and 4. A rotation by 180 degrees is the element of S_4 given by

$$\rho \ = \ (1\ 3)(2\ 4) \quad .$$

A reflection through one line of symmetry is given by

$$\tau \ = \ (1\ 2)(3\ 4) \quad .$$

Notice that

$$\rho\tau \ = \ (1\ 4)(2\ 3) \qquad \textit{and} \qquad \tau\rho \ = \ (1\ 4)(2\ 3)$$

and so $\rho\tau = \tau\rho$. Furthermore ,

$$\rho^2 = e, \qquad \tau^2 = e, \qquad (\rho\tau)^2 = \rho^2\tau^2 = ee = e \quad .$$

The set $V = \{\ e,\ \rho,\ \tau,\ \rho\tau\ \}$ is a subgroup of S_4. It is easily seen to be closed under the group operation of S_4. Most cases are obvious. Two cases that are not immediately obvious are

$$\rho(\rho\tau) = \rho^2\tau = e\tau = \tau, \qquad (\rho\tau)\rho = \rho(\tau\rho) = \rho(\rho\tau) = \rho^2\tau = e\tau = \tau$$

and similarly, $\tau(\rho\tau) = (\rho\tau)\tau = \rho$. These products are in V.

The subgroup V of S_4 is quite important. It is explicity given by

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

The subgroup V is called the Klein Four-Group.

8. Determine the center of the group Q_8. Determine the center of the group D_4. Determine the center of the group $G = A \times B$, where A and B are groups of order 4.

Solution. The center of Q_8 is $\{1,\ -1\}$. One checks easily that $\pm i,\ \pm j$ and $\pm k$ are not in $Z(Q_8)$. For example, $i \notin Z(Q_8)$ because $ij \neq ji$.

The center of D_4 is $\{e,\ \rho\}$, where ρ is the element of D_4 mentioned in the solution to problem 7. One checks easily that $\rho\sigma = \sigma\rho$ for all $\sigma \in D_4$. One checks easily that the remaining six elements of D_4 are not in $Z(D_4)$.

Finally, the groups A and B of order 4 must be abelian (as proved in class). Hence $G = A \times B$ is abelian. Hence, the center of G is G itself.