Solutions for the Midterm

QUESTION 1. Let σ and τ be the following two elements in S_9:

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

Since S_9 is a group, we have $\sigma\tau \in S_9$.

(a) Express $\sigma\tau$ as a product of disjoint cycles.

Solution. We will determine the orbits. We must apply the bijection τ first and then σ. Here are the orbits:

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

It follows that

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

This expresses $\sigma\tau$ as a product of disjoint cycles.

(b) Determine the orders of σ, τ, and $\sigma\tau$.

Solution. The cycle decomposition of an element in S_n determines the order of the element. The order is the least common multiple of the lengths of the cycles occurring in the cycle decomposition. Thus, the orders of σ, τ, and $\sigma\tau$ are 2, 20, and 6, respectively.

(c) Let $H = \langle\tau\rangle$. How many elements in H have order 5? How many elements in H have order 6?

Solution. We know that $|H| = |\tau|$. Since $|\tau| = 20$, it follows that H is a cyclic group of order 20. Note that 5 divides $|H|$. Since H is cyclic, H has exactly one subgroup K of order 5. If $h \in H$ and $|h| = 5$, the $\langle h\rangle$ is a subgroup of H of order 5. Therefore, $\langle h\rangle = K$. Thus, we must determine the number of elements in K of order 5. The identity element has order 1. Each of the remaining elements if K must have order dividing 5 and hence must have order 5. There are four such elements. It follows that H has exactly four elements of order 5.

Recall that we proved the following result: *If G is a finite, abelian group and $a \in G$, then $|a|$ divides $|G|$.* We can apply this result to the cyclic group H since H is abelian. Since

6 does not divide $|H| = 20$, there cannot be any elements in H of order 6. Thus, the number of elements of H of order 6 is zero.

QUESTION 2. Suppose that G is an abelian group. Suppose that $a,\ b \in G$.

(a) Carefully prove that if $|a| = 9$ and $|b| = 27$, then $|ab| = 27$.

Solution. Since G is abelian, we have $(ab)^k = a^k b^k$ for any $k \in \mathbf{Z}$. We proved this in the solution of a homework problem. By assumption, we have $a^9 = e$ and $b^{27} = e$, where e is the identity element of G. It follows that

$$(ab)^{27} \;=\; a^{27}b^{27} \;=\; (a^9)^3 b^{27} \;=\; e^3 e \;=\; e$$

and therefore $|ab|$ must divide 27. We are using proposition 5 on the handout about cyclic groups and orders of elements. Let $m = |ab|$. Thus, we have $m \in \{1,\ 3,\ 9,\ 27\}$.

To prove that $m = 27$, it suffices to show that $m \notin \{1,\ 3,\ 9\}$. Equivalently, we must show that m does not divide 9. By proposition 5 (again), it suffices to show that $(ab)^9 \neq e$. Note that

$$(ab)^9 \;=\; a^9 b^9 \;=\; eb^9 \;=\; b^9 \;\neq\; e$$

Here we have used the fact that $|a| = 9$ (and so $a^9 = e$) and the fact that $b^9 \neq e$ which is true because $0 < 9 < 27 = |b|$.

We have proved that $|ab| = 27$.

(b) Give a specific example of an abelian group G and two specific elements $a,\ b \in G$ such that $|a| = 9,\ |b| = 9$, and $|ab| = 3$.

Solution. Let G be a cyclic group of order 9. Let a be a generator of G. Thus, $a \in G$ and $|a| = 9$. We know that G has a cyclic subgroup H of order 3 since 3 divides 9. In fact, as proved in class, $H = \langle c \rangle$, where $c = a^t$ and $t = 9/3 = 3$. That is, $c = a^3$. We can find a $b \in H$ so that $ab = c$. Namely, $b = a^{-1}c = a^{-1}a^3 = a^2$. Since a has order 9 and $gcd(2, 9) = 1$, it follows that $b = a^2$ also has order 9. We are using proposition 8 on the handout about cyclic groups and orders of elements. Thus, we have

$$|a| = 9, \qquad |b| = 9, \qquad |ab| = |c| = 3$$

as we wanted.

QUESTION 3. No justifications are needed in this question. One can either give a specific example of a group with the stated property or say that no such group exists.

We will give justifications in the solutions below even though the question does not require justifications.

(a) Give a specific example (if possible) of a group A which has exactly seven elements of order 2.

Solution. We can take $A = A_1 \times A_2 \times A_3$, where

$$A_1 \;=\; A_2 \;=\; A_3 \;=\; \{1, \;-1\} \;\;.$$

Then $|A| = 8$. Furthermore, every element $a \in A$ is of the form $a = (a_1,\; a_2,\; a_3)$, where a_1, a_2, and a_3 have orders 1 or 2. It follows that a^2 is equal to the identity element in A. Of course, the identity element in A has order 1. The remaining seven elements in A have order 2.

One could also choose $A = A_1 \times A_2 \times A_3$, where $A_1,\; A_2$ and A_3 are any finite cyclic groups of even order.

Some other possible choices of A are $A = D_6$ (which is the group of symmetries of a regular hexagon) or $A = D_7$ (which is the group of symmetries of a regular 7 sided polygon).

(b) Give a specific example (if possible) of a group B which has exactly five elements of order 2.

Solution. One choice is $B = D_4$, the group of symmetries of a square. That group has four reflections (each of which has order 2). The set of rotations in D_4 is a cyclic subgroup of D_4 of order 4 and has a unique element of order 2. Thus, D_4 indeed has exactly five elements of order 2.

Another choice is $B = D_5$ (which is the group of symmetries of a regular pentagon). It has five reflections (each of which has order 2). The subgroup of rotations has order 5 and cannot contain an element of order 2.

(c) Give a specific example (if possible) of a group C which has exactly five elements of order 4.

Solution. No such group C exists. To see this note that if $a \in C$ has order 4, then a^{-1} also has order 4. Furthermore, $a^{-1} \neq a$ because $|a| \neq 2$. Thus, we can partition the set of elements of order 4 in any group into pairs $\{a,\ a^{-1}\}$. It is not hard to verify that any two such pairs are disjoint (unless they coincide). Thus, the set of elements of order 4 (if finite) must have even cardinality.

(d) Give a specific example (if possible) of a group D which has exactly four elements of order 5 and exactly six elements of order 7.

Solution. Let D be a cyclic group of order 35. We know that D contains a unique subgroup H of order 5, that H is cyclic, and that any element in D of order 5 must generate that subgroup H. Thus, H (and hence D) contains exactly four elements of order 5. Furthermore, we know that D contains a unique subgroup K of order 7, that K is cyclic, and that any element in D of order 7 must generate that subgroup K. Thus, K (and hence D) contains exactly six elements of order 7.

A specific example is $D = \langle \sigma \rangle$, where σ is the following element in S_{12}:

$$\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)(8\ 9\ 10\ 11\ 12)\quad .$$

A simpler example is $D = \mathbf{Z}_{35}$ under the operation of addition.

(e) Give a specific example (if possible) of an abelian group E of order 35 which is not a cyclic group.

Solution. No such group E exists. It turns out that a group E of order 35 must have at least one element a of order 5 and at least one element b of order 7. We will explain why below. If the group E is abelian, then $ab = ba$. One can verify that $(ab)^{35} = e$, where e is the identity element in E. Thus $|ab|$ must divide 35. Thus, $|ab|$ is in the set $\{1,\ 5,\ 7,\ 35\}$. One can also verify that $(ab)^5 \neq e$ and $(ab)^7 \neq e$. Thus, $|ab|$ is not in the set $\{1,\ 5,\ 7\}$. It follows that $|ab| = 35$. Thus, E contains an element of order 35, namely ab. If E has order 35, then $E = \langle ab \rangle$. Thus, E is actually a cyclic group, contrary to what we want.

To explain why E must have an element of order 5 and an element of order 7, assume to the contrary that E has no element of order p, where $p = 5$ or $p = 7$. The order of an element in E must divide $|E| = 35$. We consider $p = 5$ first. Then E cannot have an element of order 35 since 5 divides 35. Thus, every element of E has order 7, except for the identity element. Thus, E has exactly 34 elements of order 7. However, every element of order 7 generates a unique cyclic subgroup of order 7. The other elements in that subgroup (except for e) generate the same subgroup. Thus, if there are k cyclic subgroups of order 7, there will be $6k$ elements of order 7. Thus, we would have $6k = 34$ which is impossible. Similarly, if $p = 7$, then every nonidentity element in E has order 5. If k denotes the number of cyclic subgroups of order 5, we would have $4k = 34$. That is also impossible. It follows that E must have at least one element a of order 5 and at least one element b of order 7, as stated above.