Math 212, Assignment 2 - SOLUTIONS

All questions are equally weighted. They will be marked for correctness and clarity of explanation.

1. (a) Let G and H be groups, with $g \in G$ and $h \in H$. Prove that the order of (g, h) in $G \oplus H$ is the least common multiple of $o(g)$ and $o(h)$.

Solution. [Note: the least common multiple of two integers is only defined for finite numbers; therefore we restrict to elements g and h of finite order.]

Let e_G and e_H be the identity elements of G and H, respectively.

Suppose there exists $c \in \mathbb{Z}+$ such that $(g, h)^c = (e_G, e_H)$. Then $g^c = e_G$ and $h^c = e_H$. The first of these implies that c is a multiple of $o(g)$ and the second implies that c is a multiple of $o(h)$. That is, c is a common multiple of $o(g)$ and $o(h)$. We have shown that if c is a positive integer satisfying $(g, h)^c$ then c is a common multiple of $o(g)$ and $o(h)$. On the other hand, by defintion, the order of (g, h) is the least positive integer satisfying $(g, h)^c$. By the above observation, we conclude *if* the order of (g, h) is finite, then it is the least common multiple of $o(g)$ and $o(h)$; let's call this number n. It remains to show that n is actually the order of (g, h) in $G \oplus H$.

Since n is a multiple of $o(g)$ (that is, $n = ko(g)$ for some $k \in \mathbb{Z}$) and a multiple of $o(h)$ (that is, $n = \ell o(h)$ for some $\ell \in \mathbb{Z}$), we have

$$(g, h)^n = (g^n, h^n) = (g^{ko(g)}, h^{\ell o(h)}) = ((g^{o(g)})^k, (h^{o(h)})^\ell) = (e_G^k, e_H^\ell) = (e_G, e_H).$$

This completes the proof.

(b) For which pairs of natural numbers m and n is $\mathbb{Z}_m \oplus \mathbb{Z}_n$ cyclic? Explain.

Solution. We claim that $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic if and only if m and n are relatively prime.

Proof: First, note that if (g, h) is a generator of $G \oplus H$ then g is a generator of G and h is a generator of H, so let (g, h) be an element of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ such that g is a generator of $\mathbb{Z}_m$ and h is a generator of $\mathbb{Z}_n$. We will show that (g, h) is a generator of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ if and only if m and n are relatively prime. (In the case where (g, h) is not a generator, it follows from the above that no generator exists.)

Since g is a generator of $\mathbb{Z}_m$ and h is a generator of $\mathbb{Z}_n$, we have $o(g) = m$ and $o(h) = n$, by Corollary 3.6.9. By part (a), the order of (g, h) in $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is $\text{lcm} m, n$. Recall that $\text{lcm}(m, n) = \frac{mn}{\gcd(m,n)}$, for any natural numbers m and n. Therefore

$o((g,h)) = \frac{mn}{\gcd(m,n)}$, which equals mn, the order of the group $\mathbb{Z}_m \oplus \mathbb{Z}_n$, if and only if $\gcd(m,n) = 1$. Therefore, by Corollary 3.6.9, (g,h) is a generator of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ if and only if m and n are relatively prime.

2. In S_{12}, let $\sigma = (5\ 11)$ and $\pi = (3\,4\,5\,6)$.

(a) Compute

$$\sigma^{-1}\pi\sigma,$$

writing the answer as a product of disjoint cycles.

Solution. $\sigma^{-1}\pi\sigma = (3\,4\,11\,6)$

(b) Based on part (a), find $\tau \in S_{12}$ such that

$$\tau^{-1}\pi\tau = (9\ 10\ 11\ 12).$$

Solution. One example is $\tau = (3\,9)(4\,10)(5\,11)(6\,12)$. However, there are many examples that will work: τ can be any permutation in S_{12} that sends 9 to 3, 10 to 4, 11 to 5 and 12 to 6. We will prove this in part (c).

(c) Let $(a_1\,a_2\,\ldots a_k)$ and $(b_1\,b_2\,\ldots b_k)$ be cycles in S_n. Give a permutation $\tau \in S_n$ that satisfies

$$\tau^{-1}(a_1\,a_2\ldots a_k)\tau = (b_1\,b_2\,\ldots b_k),$$

and explain why your choice of τ works.

Solution. Let τ be any permutation of S_n such that $\tau(b_i) = a_i$ for $i = 1,\ldots,k$. Then $\tau^{-1}(a_i) = b_i$ for $i = 1,\ldots,k$.
Let $\pi = (a_1\,a_2\,\ldots a_k)$. Then $\pi(a_i) = a_{i+1}$ for $i = 1,\ldots,k-1$, and $\pi(a_k) = a_1$.
Therefore for $i = 1,\ldots,k-1$, we have

$$\begin{aligned} \tau^{-1}\pi\tau(b_i) &= \tau^{-1}\pi(a_i) \quad \text{by definition of } \tau \\ &= \tau^{-1}(a_{i+1}) \\ &= b_{i+1} \end{aligned}$$

and (consider the case $i = k$ separately, because of the "wrap around"),

$$\begin{aligned} \tau^{-1}\pi\tau(b_k) &= \tau^{-1}\pi(a_k) \\ &\tau^{-1}(a_1) \\ &= b_1. \end{aligned}$$

We have shown that $\tau^{-1}\pi\tau$ sends

$$\begin{aligned} &b_1 \text{ to } b_2, \\ &b_2 \text{ to } b_3, \\ &\quad\vdots \\ &b_{k-1} \text{ to } b_k, \quad \text{and} \\ &b_k \text{ to } b_1. \end{aligned}$$

This implies that the disjoint cycle representaiton of $\tau^{-1}\pi\tau$ contains the cycle $(b_1\, b_2\, \ldots b_k)$. It remains to show that it does not contain any other cycle. To prove this, we will show that for all $c \neq b_1, b_2, \ldots, b_k$, in $\{1, 2, \ldots, , n\}$, $\tau^{-1}\pi\tau$ fixes c: that is, $\tau^{-1}\pi\tau(c) = c$.

Note that for these elements c, $\tau(c) \neq a_1, a_2 \ldots, a_k$, so π fixes $\tau(c)$: that is, $\pi\tau(c) = \tau(c)$. Therefore,

$$\tau^{-1}\pi\tau(c) = \tau^{-1}\tau(c) = c,$$

as required.

It follows that $\tau^{-1}\pi\tau$ is the permutation whose disjoint cycle representation is the single cycle $(b_1\, b_2\, \ldots b_k)$.

3. For $n \geq 2$, let A_n be the subset of S_n consisting of all even permutations in S_n. Prove that A_n is a group.

Solution. We first show that composition is a binary operation on A_n. Let σ and π be two elements of A_n. Then each of them is a permutation in S_n that can be written as a product of evenly many transpositions. Suppose σ can be written as a product of q transpositions and π can be written as a product of r transpositions (where q and r are both even). Then $\sigma\pi$ is a permutation in S_n, since composition is a binary operation on S_n. Moreover, $\sigma\pi$ can be written as a product of $q + r$ transpositions (in particular, it can be written as a product of the q transpositions of σ composed with the r transpositions of π). Since q and r are even, $q + r$ is even. Therefore, $\sigma\pi$ is in A_n.

Since composition is associative on S_n, it is associative on any subset of S_n; in particular it is associative on A_n.

To see that the identity permutation is even, note that $\varepsilon = (1\,2)(1\,2)$; that is, it can be written as a product of two transpositions.

Finally, we will show that every element of A_n has an inverse in A_n. Let σ be an arbitrary element of A_n. Then σ can be written as $\sigma = \tau_1\tau_2 \ldots \tau_r$, where r is even and $\tau_1, \ldots, \tau_r$ are transpositions. We claim that $\tau_r\tau_{r-1}\ldots\tau_1$ is an inverse of σ. Indeed, since every transposition is its own inverse, we have

$$\begin{aligned}
\sigma\tau_r\tau_{r-1}\ldots\tau_1 &= \tau_1\tau_2\ldots\tau_{r-1}\tau_r\tau_r\tau_{r-1}\ldots\tau_1 \\
&= \tau_1\tau_2\ldots\tau_{r-1}\varepsilon\tau_{r-1}\ldots\tau_1 \\
&= \tau_1\tau_2\ldots\tau_{r-2}\tau_{r-1}\tau_{r-1}\tau_{r-2}\ldots\tau_1 \\
&= \tau_1\tau_2\ldots\tau_{r-3}\tau_{r-2}\tau_{r-2}\tau_{r-3}\ldots\tau_1 \\
&\vdots \\
&= \tau_1\tau_1 \\
&= \varepsilon.
\end{aligned}$$

Therefore σ^{-1} can be written as a product of r transpositions, and r is even, so $\sigma^{-1} \in A_n$.

We have shown that composition is an associative binary operation on A_n, that A_n contains an identity for composition, and that every element of A_n has an inverse (also in A_n). Therefore A_n is a group with composition.

4. Let $n \geq 2$. Show that exactly half of the permutations in S_n are even by finding a bijection from the set of all even permutations in S_n to the set of all odd permutations in S_n.

Solution. Let A_n be the set of all even permutations in S_n and B_n be the set of all odd permutations in S_n (so $B_n = S_n \setminus A_n$). Consider a permutation σ in A_n. Since σ is the product of an even number of tranpositions, composing σ with a single transposition will produce an odd permutation. With this in mind, we define $f : A_n \to B_n$ by $f(\sigma) = \sigma \cdot (1\,2)$ (that is, σ composed with the transposition $(1\,2)$). We will show that f is a bijection. The easiest way to do this is to show that f has an inverse. Actually, it happens that f is its own inverse. To see this, note that

$$\begin{aligned}
f(f(\sigma) &= f(\sigma \cdot (1\,2)) \\
&= (\sigma \cdot (1\,2)) \cdot (1\,2) \\
&= \sigma \cdot ((1\,2) \cdot (1\,2)) \\
&= \sigma \cdot \varepsilon \\
&= \sigma.
\end{aligned}$$

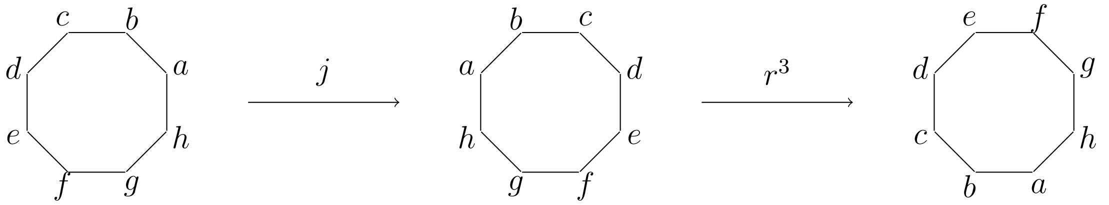
Since there is a bijection between A_n an B_n, we have $|A_n| = |B_n|$. It follows that A_n contains exactly half of the elements of S_n.

5. In the group D_8, give an algebraic proof that r^3j has order 2, and also a geometric proof of the same fact.

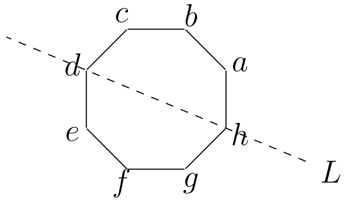
Solution. For the algebraic proof, note that

$$\begin{aligned}(r^3j)^2 &= (r^3j)(r^3j) & \\ &= r^3jjr^{8-3} & \\ &= r^3r^5 & \text{since } j^2 = \varepsilon \\ &= \varepsilon & \text{since } r^8 = \varepsilon.\end{aligned}$$

For the geometric proof, recall that the group D_8 is the group of symmetries of a regular octagon. The symmetry j is a flip over a vertical line through the centre of the octagon, and r^3 is a counterclockwise rotation of $3 \times \frac{360}{8} = 135$ degrees. Therefore, performing j and then r^3 does the following to the octagon:



This has the same result as reflecting the octagon over the line L indicated below:



Therefore r^3j is a flip, so performing r^3j twice returns the octagon to its original orientation. It follows that $(r^3j)^2 = \varepsilon$, and so $o(r^3j) = 2$.

6. For $n \geq 4$, is D_n cyclic? Explain your answer.

Solution. No. Every cyclic group is abelian and D_n is not abelian.

7. (a) How many generators does the group $\mathbb{Z}_{15}$ have?

Solution. By Corollary 3.6.9, $[k]_{15}$ is a generator of $\mathbb{Z}_{15}$ if and only if $[k]_{15}$ has order 15. Since the order of $[k]_{15}$ is $\frac{15}{\gcd(15,k)}$, this means $[k]_{15}$ is a generator if and only if $\gcd(15, k) = 1$. It follows that $[k]_{15}$ is a generator if and only if k is not divisible by 3 or 5. We can assume without loss of generality that $0 \leq k \leq 14$.

Among these integers, the ones that *are* divisible by 3 or 5 are 0, 3, 5 and 6, 9, 10, and 12. Therefore the other eight elements $[k]_{15}$ are all generators.

(b) Let p and q be distinct primes. How many generators does the group $\mathbb{Z}_{pq}$ have?

Solution. By Theorem 3.2.8, the order of $[k]_{pq}$ is $\frac{pq}{d}$, where $d = \gcd(pq, k)$. Therefore $[k]$ is a generator of $\mathbb{Z}_{pq}$ if and only if $\gcd(pq, k) = 1$. We may assume that $0 \leq k \leq pq - 1$; we must determine how many of these integers are relatively prime to pq. Since p and q are prime, the only integers in $\{0, 1, \ldots, pq-1\}$ that are *not* relatively prime with pq are those that are divisible by p or divisible by q (or both). We will use the Principle of Inclusion/Exclusion to count these integers.

Let P denote the set of integers from $\{0, 1, \ldots, pq-1\}$ that are divisible by p, and Q denote the set of integers from $\{0, 1, \ldots, pq-1\}$ that are divisible by q. We want $\#(P \cup Q)$, and by the PIE, this is equal to $\#(P) + \#(Q) - \#(P \cap Q)$. Since every p^{th} integer is divisible by p, in any set of pq consecutive integers (such as the set $\{0, 1, \ldots, pq-1\}$) there are exactly q that are divisible by p. Therefore $\#(P) = q$. Similarly, $\#(Q) = p$. The set $P \cap Q$ contains the integers that are divisible by both p and q; that is, the integers that are divisible by pq. The only such integer in the given set is 0, so $\#(P \cap Q) = 1$. Therefore $\#(P \cup Q) = p + q - 1$. Since this is the number of integers in $\{0, 1, \ldots, pq - 1\}$ that are *not* relatively prime to pq, the number that *are* relatively prime to pq is $pq - (p + q - 1) = pq - p - q + 1$. Therefore the group $\mathbb{Z}_{pq}$ has $pq - p - q + 1$ generators.

8. Is U_{10} cyclic? Is U_{12}? For each, find a generator or prove that it is not cyclic.

Solution. First we find the elements of U_{10} and U_{12}.

In $\mathbb{Z}_{10}$, the elements [1], [3], [7] and [9] have inverses for multiplication, since

$$[1]_{10}[1]_{10} = [1]_{10}, \quad \text{and} \quad [3]_{10}[7]_{10} = [21]_{10} = [1]_{10} \quad \text{and} \quad [9]_{10}[9]_{10} = [81]_{10} = [1]_{10}.$$

It is also easy to verify that the other elements do not have an inverse for multiplication:

- $[0]_{10}[k]_{10} = [0]_{10}$ for all k,
- each of $[2]_{10}[k]_{10}$, $[4]_{10}[k]_{10}$, $[6]_{10}[k]_{10}$ and $[8]_{10}[k]_{10}$ is in $\{[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}$ for all k, and
- $[5]_{10}[k]_{10} \in \{[0]_{10}, [5]_{10}\}$ for all k.

We claim that $[3]_{10}$ is a generator of U_{10}. Indeed,

$$[3]^2 = [9]$$

$$[3]^3 = [9][3] = [27] = [7]$$

$$[3]^4 = [7][3] = [21] = [1],$$

(omitting the subscript "10"). Therefore U_{10} is cyclic.

On the other hand, we claim that U_{12} is not cyclic. We have

$$U_{12} = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\},$$

which can be verified using the same method we used for U_{10}. We will show that none of these elements has order 4. From now on we omit the subscript "12".

Clearly $o([1]) = 1$, since $[1]$ is the identity for multiplication.
Since $[5]^2 = [25] = [1]$ (in $\mathbb{Z}_{12}$), we have $o([5]) = 2$.
Similarly, $[7]^2 = [49] = [1]$ (in $\mathbb{Z}_{12}$), so $o([7]) = 2$.
Finally, $[11]^2 = [121] = [1]$ (in $\mathbb{Z}_{12}$), so $o([11]) = 2$.
Therefore no element of U_{12} has order 4, so no element is a generator. It follows that U_{12} is not cyclic.

Rules for group assignments. Make sure you follow the universal rules for group assignments (below) and any additional rules/procedures laid out in your Group Contract.

1. Each group member is expected to contribute to the best of their ability, and assignment submissions should only include the names of group members who meet this expectation.

2. Each group member should be able to explain the group's solution to me and answer any questions I may have about it. It is the whole group's responsibility to ensure that this standard is met.

3. The task of composing final solutions and writing them up in good copy must be shared equally among all group members (after a collaborative problem-solving process).

4. After good copy solutions are complete, they should be shared among all group members to be double-checked and proofread. This should be done in advance of the due date, to allow time for any necessary corrections. Corrections should be completed by the person who wrote the original solution.