Midterm solutions

I. Short questions

Problem 1. State the First Isomorphism Theorem for groups.

Theorem 1. Let $f\colon G \to H$ be a group homomorphism. Then $\ker f \trianglelefteq G$ and $G/\ker f \cong \operatorname{im} f$.

Problem 2. For each of the questions below, give an example with the required properties. No explanations required.

(a) A group that is not cyclic.

Solution 1. There are many correct answers.

Here are some examples: D_4 (or D_n for any $n \geqslant 3$), $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) A group G that is not abelian and a subgroup H of G that is abelian.

Solution 2. D_4 and the subgroup $\{e, s\}$.

Problem 3. For each of the questions below, give an example with the required properties, and briefly explain why the required properties are satisfied.

(a) A group G and a subgroup H that is *not* normal in G.

Solution 3. Let $G = D_4$ and consider the subgroup $H = \{e, s\}$. Note that H is not a normal subgroup, since we showed in class that $srs = r^{-1} = r^3$, and since $s = s^{-1}$ we have

$$rs = sr^{-1} \implies rsr^{-1} = sr^{-1}r^{-1} = sr^{-2}.$$

(b) Two groups G and H of the same finite order that are *not* isomorphic.

Solution 4. The groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ both have order 4 but are not isomorphic, since $\mathbb{Z}_4$ is cyclic and thus has an element of order 4, while every nontrivial element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2.

Problem 4. Find (with proof!) the order of $(23)(5689)$ in S_{10}.
You can freely use any results we might have proved about this.

Solution 5. We proved in class that k-cycles have order k, so $|(23)| = 2$ and $|(5689)| = 4$. We also showed in a problem set that if σ and τ are disjoint cycles, then $|\sigma\tau| = \operatorname{lcm}(|\sigma|, |\tau|)$, and since (23) and (5689) are disjoint cycles, we conclude that

$$|(23)(5689)| = \operatorname{lcm}(|(23)|, |(5689)|) = \operatorname{lcm}(2, 4) = 4.$$

II. Old problems

Choose **2** of the following problems.

Problem 5. Let $f\colon G \to H$ be a group homomorphism. Show that $\ker f$ is a normal subgroup of G. Note: You must show *both* that $\ker f$ is a subgroup of G and that it is normal.

Proof. First, we need to show that $\ker f$ is a subgroup of G. Since $f(e) = e$, we have $e \in \ker f$, and in particular $\ker f$ is nonempty. Moreover, given $g, h \in \ker(f)$,

$$f(gh^{-1}) = f(g)f(h)^{-1} = ee^{-1} = e,$$

so $gh^{-1} \in \ker f$. By the One-Step Test, $\ker f$ is a subgroup of G.

Now we need to show this is a normal subgroup of G. Given any $g \in G$ and any $h \in \ker f$,

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g) \cdot e \cdot f(g)^{-1} = f(g)f(g)^{-1} = e.$$

Therefore, $ghg^{-1} \in \ker f$, and we conclude that $\ker f$ is a normal subgroup of G. $\square$

Problem 6. Let G be a group and H and H' subgroups of G. Prove that $H \cup H'$ is a subgroup of G if and only if $H \subseteq H'$ or $H' \subseteq H$.

Proof. ($\Leftarrow$) If $H \subseteq H'$ or $H' \subseteq H$, then we either have $H \cup H' = H$ or $H \cup H' = H'$, which are both subgroups.

($\Rightarrow$) Suppose by way of contradiction that $H \cup H'$ is a subgroup but $H \not\subseteq H'$ and $H' \not\subseteq H$. Choose $a \in H \setminus H'$ and $b \in H' \setminus H$. Then $a, b \in H \cup H'$, and since $H \cup H'$ must be closed for the multiplication, we conclude that $ab \in H \cup H'$. But if $ab \in H$, then multiplying on the left by a^{-1} gives $b = a^{-1}(ab) \in H$, a contradiction. A similar contradiction holds if $ab \in H'$, giving us $a = (ab)b^{-1}$. Thus $ab \notin H \cup H'$. $\square$

Problem 7. Let G be any group. Show that if $G/\operatorname{Z}(G)$ is cyclic, then G is abelian.

Proof. Let $Z := \mathbb{Z}(G)$ and suppose $G/Z = \langle xZ \rangle$ for some $x \in G$. Let $a, b \in G$. Then $aZ = x^iZ$ and $bZ = x^jZ$ for some i, j. Hence, $a = x^i z_1$ and $b = x^j z_2$ for some $z_1, z_2 \in G$. Then

$$ba = (x^j z_2)(x^i z_1) = x^{j+i} z_1 z_2 = (x^i z_1)(x^j z_2) = ab.$$

Therefore, G is abelian. $\square$

III. New problems

Choose any **2** of the following problems.

Problem 8. Let G be a group (not necessarily finite) such that every element $g \in G$ satisfies $g^2 = e$. Show that G is abelian.

Proof. Given any $g \in G$, since $g^2 = e$ then $g = g^{-1}$. Let $x, y \in G$. We have $x^{-1} = x$, $y^{-1} = y$, and $(yx)^{-1} = yx$. Moreover,

$$\begin{aligned} xy &= x^{-1}y^{-1} && \text{since } x = x^{-1} \text{ and } y = y^{-1} \\ &= (yx)^{-1} \\ &= yx && \text{since } (yx)^{-1} = yx. \end{aligned}$$

Thus $xy = yx$, and G is abelian. $\square$

Problem 9. In this problem, you can use without proof that every finite cyclic group of order n is isomorphic to $\mathbb{Z}/n$.

(a) Show that any group of prime order p is cyclic, and thus it must be isomorphic to $\mathbb{Z}/p$.

Proof. Suppose that G is a group of order p, where p is prime. Since $p \geqslant 2$, then G has at least one nontrivial element $g \in G$. By Lagrange's Theorem, the order of g must divide the order of G, but $|G|$ is prime and $|g| \neq 1$, so $|g| = |G| = p$. But $|\langle g \rangle| = |g| = p$, so $\langle g \rangle = G$. We conclude that G is cyclic and generated by g. Since every cyclic group of order p is isomorphic to $\mathbb{Z}/p$, we conclude that $G \cong \mathbb{Z}/p$. □

(b) Now suppose that G is any nontrivial group, not necessarily finite. Show that G has no nontrivial proper subgroups if and only if G is finite of order p, where p is prime.

Proof. ($\Leftarrow$) Suppose that G is a finite group of order p. We showed in part (a) that $G \cong \mathbb{Z}/p$. Let us write $[i]$ for the class of i in $\mathbb{Z}/p$.

Suppose that H is any nontrivial subgroup of G. Then H contains some nontrivial element of G, say $[i]$, where we can take $1 \leqslant i < p$. In particular, $\gcd(i,p) = 1$, so there exist integers a, b such that $ai + bp = 1$, and thus

$$[1] = a[i] \in \langle [a] \rangle \subseteq H.$$

We conclude that $H = G$.

($\Rightarrow$) Suppose that G is nontrivial but has no nontrivial subgroups. Let $g \in G$ be any nontrivial element in G. Then $\langle g \rangle$ is a nontrivial subgroup of G, and so we must have $\langle g \rangle = G$. In particular, G is cyclic. Now if G is infinite, then g must have infinite order. We showed in a problem set that all the powers g^n with $n \geqslant 0$ are distinct; in particular, $g \notin \langle g^2 \rangle$, so $\langle g^2 \rangle$ is a proper nontrivial subgroup of G. Thus G must be finite.

So we have shown that G must be a finite cyclic group, and thus $G \cong \mathbb{Z}/n$ for some n. If n is not prime, then we can write $n = ab$ for some integers $1 < a, b < n$. In particular, $b[a] = [0]$, and thus $[a]$ has order at most b, and $|\langle [a] \rangle|$ has at most b elements, so $\langle [a] \rangle \neq G$. On the other hand, $\langle [a] \rangle$ is nontrivial since it contains $[a] \neq [0]$. Thus $\langle [a] \rangle$ is a proper nontrivial subgroup. □

Problem 10. Show that there is no surjective group homomorphism $f\colon S_5 \longrightarrow S_4$.

Proof 1. Suppose that $f\colon S_5 \longrightarrow S_4$ is a surjective group homomorphism. By the First Isomorphism Theorem,

$$S_4 \cong S_5 / \ker f.$$

Moreover, Lagrange's Theorem now tells us that

$$\frac{|S_5|}{|\ker f|} = |S_4| \implies |\ker f| = \frac{|S_5|}{|S_4|} = \frac{5!}{4!} = 5.$$

Thus $|\ker f| = 5$, and by 9(a), $\ker f$ must be cyclic. Consider any generator g for $\ker f$, which must then be an element of order 5.

Every element in S_5 can be written uniquely as a product of disjoint cycles, and its order is the least common multiple of the orders of each cycle. Moreover, any k-cycle has order k and the only element of order 1 is the identity. Since 5 is prime, g must be a product of 5-cycles; but we have only 5 elements to order, so we conclude that g must be a cycle of order 5.

Without loss of generality, assume $g = (12345)$; we can always rename the elements as such. So $\ker f = \langle (12345) \rangle$. Now the kernel of a homomorphism must be a normal subgroup, but we claim that $\langle (12345) \rangle$ is not a normal subgroup of S_5. On the one hand,

$$\langle (12345) \rangle = \{e, \underset{g}{(12345)}, \underset{g^2}{(13524)}, \underset{g^3}{(13524)}, \underset{g^4}{(15432)}\}.$$

But if we take, for example, $\sigma = (12)$, then by a formula from a problem set we know that

$$\sigma(12345)\sigma^{-1} = (\sigma(1)\,\sigma(2)\,\sigma(3)\,\sigma(4)\,\sigma(5)) = (21345) \notin \langle (12345) \rangle.$$

We conclude that $\langle (12345) \rangle$ is not a normal subgroup of S_5, and thus no such f can exist. $\square$

Proof 2. Suppose that $f \colon S_5 \longrightarrow S_4$ is any group homomorphism, and let σ be a 5-cycle. The σ has order 5, and thus

$$f(\sigma)^5 = f(\sigma^5) = f(e) = e,$$

so the order of $f(\sigma)$ divides 5. Since 5 is prime, $f(\sigma) = e$ or $|f(\sigma)| = 5$. However, we claim that there are no elements of order 5 in S_4, which means that $f(\sigma) = e$. To see that, recall that every element τ of S_4 can be written uniquely as a product of disjoint cycles $\tau = \tau_1 \cdots \tau_k$, and $|\tau| = \operatorname{lcm}(|\tau_1|, \ldots, |\tau_k|)$. But a k-cycle has order k, and thus a cycle in S_4 can only have order $1, 2, 3$, or 4. In particular, the lcm of any subset of the integers $\{1, 2, 3, 4\}$ cannot equal 5, so S_4 has no elements of order 5.

We conclude that every 5-cycle in S_5 is in the kernel of f. Let's count the number of 5-cycles. There are 5! ways to order the numbers $1, 2, 3, 4, 5$, but since permuting our list cyclicly will still correspond to the same cycle, there are $\frac{5!}{5} = 4!$ elements of S_5 that are 5-cycles. In particular, $|\ker f| \geqslant 4!$.

By the First Isomorphism Theorem,

$$S_5 / \ker f \cong \operatorname{im} f.$$

Moreover, Lagrange's Theorem now tells us that

$$|\operatorname{im} f| = \frac{|S_5|}{|\ker f|} = \frac{5!}{|\ker f|} \leqslant \frac{5!}{4!} = 5.$$

In particular, it is not possible for f to be surjective. $\square$