Midterm solutions.

Problem 1. (1) Define what it means for two groups to be isomorphic.

(2) Define the order of an element of a group. Give an example to show that the order can be infinite. No proof is necessary.

Proof.

(1) Two groups G and H are isomorphic if there exists a bijective map $f : G \to H$ s.t. f is a homomorphism. That is, f is one to one, onto and satisfies $f(xy) = f(x)f(y)$ for any two elements $x, y \in G$.

(2) Let G be a group and $x \in G$. The order of x is $n \in \mathbb{Z}$ if n is the *smallest* positive number for which $x^n = e$. This is equivalent to saying that n is the order of the subgroup of G generated by x.

An example of an element of infinite order is the element 1 in the group $\mathbb{Z}$ of integers under addition.

$\square$

Problem 2. Let $G = \{1, 2, 3, 4\}$ with group law multiplication modulo 5.

(1) Describe all the subgroups of G. No proof is necessary.

(2) Describe an isomorphism ϕ from G to itself, *besides* $\phi(x) = x$. No proof is necessary.

Proof.

(1) Since any element of G other than 1 generates G, there are two subgroups: $\{e\}$ and G.

(2) An isomorphism $\phi : G \to G$ can be defined by $\phi(x) = x^{-1}$ so $\phi(1) = 1$, $\phi(2) = 3$, $\phi(3) = 3$ and $\phi(4) = 4$.

$\square$

Problem 3. Let G be a group and let A, B be subgroups of G. Set

$$C = \{a \circ b | a \in A, b \in B\}$$

(1) Prove that, if G is abelian, then C is a subgroup.

(2) Give an example to show that C *need not* be a subgroup.

Proof.

(1) Since G is a group, C is a subset of G. We need to show:

Closed under group law: Let $c = a \circ b$ and $c' = a' \circ b'$ be in C with $a, a' \in A$ and $b, b' \in B$. Then $(a \circ b) \circ (a' \circ b') = (a \circ a') \circ (b \circ b')$ since G is abelian. Since A, B are subgroups of G, $a \circ a' \in A$ and $b \circ b' \in B$. Thus $c \circ c' \in C$ so C is closed under the group law.

Identity: Since A, B are subgroups of G, $e \in A, B$. Thus $e \circ e = e \in C$.

Inverses: Let $c = a \circ b \in C$ with $a \in A, b \in B$. Since A, B are subgroups of G, we have that $a^{-1} \in A$, $b^{-1} \in B$ so $a^{-1} \circ b^{-1} \in C$. Then $(a \circ b) \circ (a^{-1} \circ b^{-1}) = (a \circ a^{-1}) \circ (b \circ b^{-1}) = e$ since G is abelian. Thus every element of C has an inverse.

Associativity: Since C is a subset of G, multiplication in C is associative.

Therefore C is a group if G is abelian.

(2) Let $G = S_3$, let $A = \{e, (12)\}$ and let $B = \{e, (13)\}$. Then $C = \{e, (12), (13), (12)(13) = (132)\}$. But C is not a subgroup of S_3 because $(132)^2 = (123)$ in not in C.

$\square$

Problem 4. (1) Let G be a group of order 27 and $x \in G$. Suppose also that x^9 is not the identity. Prove that G is cyclic.

(2) Prove that S_4 is not isomorphic to the dihedral group of order 24. [Hint: how many elements of order 3 in both groups?]

Proof.

(1) First note that x is a fixed element (so x doesn't stand for any arbitrary element of G.) The order of x divides the order of G. Since the order of G is 27, the order of x is 1, 3, 9 or 27. If the order of x were 1, 3, or 9 we could take $(x^1)^9$, $(x^3)^3$ or x^9 and see that the result would be the identity. But any of those three expressions are equal to x^9. We are given that x^9 is not the identity. So the order of x cannot be 1,3, or 9. Therefore the order of x is 27.

Take the group generated by x. It is $< x >= \{e, x, x^2, \ldots, x^{26}\}$. All of the elements in this set are distinct. There are 27 elements in $< x >$ and 27 elements in G so we must have $< x >= G$. Thus G is generated by x. Therefore G is cyclic.

(2) There are 8 elements of order 3 in S_4. They are the three-cycles (123), (132), (134), (143), (124), (142), (234), and (243).

The dihedral group of order 24 is D_{12} since D_n has $2n$ elements. D_{12} has two elements of order 2. They are r^4 and r^8. (These are the only rotations of order 3. All reflections have order 2.)

If $f : D_4 \to S_4$ were an isomorphism, it would send elements of order 3 to elements of order 3. And since f is a bijection, it would have to send distinct elements of order 3 in S_4 to distinct elements of order 3 in D_4. But the number of elements of order 3 in S_4 and D_4 are different, so there cannot be a bijection between them. So there is no isomorphism between S_4 and D_4. Therefore S_4 and D_4 are not isomorphic.

$\square$

Problem 5. Let $f : S_n \to H$ be a homomorphism where H is an abelian group.

(1) Show that if τ, τ' are transpositions, then $f(\tau) = f(\tau')$. [Hint: Briefly explain why every transposition τ is of the form $\alpha(12)\alpha^{-1}$ for some $\alpha \in S_n$.

(2) Prove that there are exactly two homomorphisms $f : S_n \to \{\pm 1\}$.

Proof.

(1) First we show the hint. Let $\tau = (ab)$ be a transposition. Let $\alpha = (1a)(2b)$ so $\alpha^{-1} = (2b)(1a)$. Then note that the element $(1a)(2b)(12)(2b)(1a)$ is actually (ab). (You can figure this out by seeing that if α sends k to k' for some k, then α^{-1} sends k' to k. If k is neither 1 nor 2, then (12) does nothing to it. And then α would put the k back to k'. So $\alpha(12)\alpha^{-1}$ only moves numbers that α^{-1} sends to 1 or 2. Then you say, I want α^{-1} to send a to 1 and b to 2, and you build such an α.) In any case, this shows that for any transposition τ there is an α s.t. $\tau = \alpha(12)\alpha^{-1}$.

Let $f : S_n \to H$ be a homomorphism. We will now show that $f(\tau) = f(12)$ for any transposition τ. From this we can conclude that $f(\tau) = f(\tau')$ for any two transpositions τ and τ'. So write $\tau = \alpha(12)\alpha^{-1}$. Then $f(\tau) = f(\alpha(12)\alpha^{-1})$. Since f is a homomorphism, this is just $f(\alpha)f(12)f(\alpha^{-1}) = f(\alpha)f(12)f(\alpha)^{-1}$. Since H is abelian, we finally get that $f(\tau) = f(12)$.

Since $f(\tau) = f(12)$ for any transposition τ, we have shown that if H is abelian, $f(\tau) = f(\tau')$.

(2) Note that $H = \{\pm 1\}$ is an abelian group. So if $f : S_n \to H$ is a homomorphism, then f sends all the transpositions to the same place. So either all the transpositions get mapped to 1, or all the transpositions get mapped to -1.

S_n is generated by transpositions. So for any $\alpha \in S_n$, α can be written as a product of transpositions. That is, $\alpha = \tau_1 \tau_2 \cdots \tau_n$ where τ_i is a transposition for all i. Since f is a homomorphism, $f(\alpha) = f(\tau_1)f(\tau_2)\cdots f(\tau_n)$. If f sends all transpositions to 1, then $f(\alpha) = 1$ for all α. If f sends all transpositions to -1, then $f(\alpha) = (-1)^n$ which is 1 if n is even and -1 if n is odd.

So there are exactly two possible homomorphisms f. The first is the one that sends every element to 1. The second is the one that sends even permutations to 1 and odd permutations to -1.

$\square$