Math 3140 — Fall 2012
Exam #2

Work alone. No materials except pen (or pencil) and paper allowed. Write your solutions on a separate paper. Justify your answers. Giving incorrect or irrelevant justification will be penalized.

Problem 1. Suppose that A, B, and C are groups with their group operations all written multiplicatively. Suppose that $\varphi : A \to B$ and $\psi : B \to C$ are homomorphisms of groups. Let $\omega = \psi \circ \varphi$. Show that the function $\omega : A \to C$ is a homomorphism of groups.

Solution. We must show that for any $x, y \in A$ we have $\omega(xy) = \omega(x)\omega(y)$. We have

$$\begin{aligned}
\omega(xy) &= \psi(\varphi(xy)) && \text{definition of } \omega \\
&= \psi(\varphi(x)\varphi(y)) && \varphi \text{ is a homomorphism} \\
&= \psi(\varphi(x))\psi(\varphi(y)) && \psi \text{ is a homomorphism} \\
&= \omega(x)\omega(y) && \text{definition of } \omega.
\end{aligned}$$

This holds for any $x, y \in A$ so ω is a homomorphism. □

Comments. Since this problem was worth 5 points and most people wrote very good answers, I only gave full credit to answers that were really perfect. You should consider a score of 4/5 quite good on this problem. □

Problem 2. Describe a group with 4 elements that is **not** isomorphic to $\mathbf{Z}/4\mathbf{Z}$. Make sure to explain how you know this group is not isomorphic to $\mathbf{Z}/4\mathbf{Z}$.

Solution. Let $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Then for every $(x, y) \in G$ we have $(x, y) + (x, y) = (2x, 2y)$ which is the same as $(0, 0)$ modulo 2. Therefore G does not contain any element of order 4. On the other hand $\mathbf{Z}/4\mathbf{Z}$ does have an element of order 4, so these groups can't be isomorphic. □

Problem 3. Let $\mathbf{R} \times \mathbf{R}$ be the group of pairs (a, b) where a and b are real numbers with group operation

$$(a, b) + (a', b') = (a + a', b + b').$$

Let $\varphi : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ be the function

$$\varphi(a, b) = a + b.$$

Show that φ is a homomorphism.

Solution. We have to check that $\varphi((a, b) + (a', b')) = \varphi(a, b) + \varphi(a', b')$. We have

$$\begin{aligned}
\varphi((a, b) + (a', b')) &= \varphi(a + a', b + b') && \text{definition of addition in } \mathbf{R} \times \mathbf{R} \\
&= a + a' + b + b' && \text{definition of } \varphi \\
&= a + b + a' + b' && \text{addition in } \mathbf{R} \text{ is commutative} \\
&= \varphi(a, b) + \varphi(a', b') && \text{definition of } \varphi.
\end{aligned}$$

□

Problem 4. Let $A = \langle 210, 360, 756 \rangle$ be the subgroup of $\mathbf{Z}$ containing $210 = 2 \cdot 3 \cdot 5 \cdot 7$ and $360 = 2^3 \cdot 3^2 \cdot 5$ and $756 = 2^2 \cdot 3^3 \cdot 7$. Recall that this means A consists of all integers of the form $210x + 360y + 756z$ with $x, y, z \in \mathbf{Z}$. List all numbers between 0 and 100 (inclusive) that are not in $\langle 210, 360 \rangle$, nor in $\langle 210, 756 \rangle$, nor in $\langle 360, 756 \rangle$. Remember to justify your answer.

Solution. First, factor the numbers:

$$\begin{aligned}210 &= 2 \cdot 3 \cdot 5 \cdot 7\\ 360 &= 2^3 \cdot 3^2 \cdot 5\\ 756 &= 2^2 \cdot 3^3 \cdot 7.\end{aligned}$$

Therefore

$$\begin{aligned}\gcd\big\{210, 360\big\} &= 2 \cdot 3 \cdot 5 = 30\\ \gcd\big\{210, 756\big\} &= 2 \cdot 3 \cdot 7 = 42\\ \gcd\big\{360, 756\big\} &= 2^2 \cdot 3^2 = 36\\ \gcd\big\{210, 360, 756\big\} &= 2 \cdot 3 = 6.\end{aligned}$$

Now,

$$\begin{aligned}\langle 210, 360\rangle &= \langle \gcd\big\{210, 360\big\}\rangle = \langle 30\rangle\\ \langle 210, 756\rangle &= \langle \gcd\big\{210, 756\big\}\rangle = \langle 42\rangle\\ \langle 360, 756\rangle &= \langle \gcd\big\{360, 756\big\}\rangle = \langle 36\rangle\\ \langle 210, 360, 756\rangle &= \langle 210, \gcd\big\{360, 756\big\}\rangle = \langle 210, 36\rangle\\ &= \langle \gcd\big\{210, 36\big\}\rangle = \langle 6\rangle.\end{aligned}$$

Therefore A contains all multiples of 6, and $\langle 210, 360\rangle$ contains all multiples of 30, and $\langle 210, 756\rangle$ contains all multiples of 42, and $\langle 360, 756\rangle$ contains all multiples of 36. Therefore we want to list all numbers between 0 and 100 that are multiples of 6 but are not multiples of 30, 42, or 36. These are:

$$\cancel{0}, 6, 12, 18, 24, \cancel{30}, \cancel{36}, \cancel{42}, 48, 54, \cancel{60}, 66, \cancel{72}, 78, \cancel{84}, \cancel{90}, 96.$$

□

Problem 5. Prove that every odd permutation in S_n has even order. (Recall that an odd permutation is one whose sign is -1.)

Solution. Let m be the order of $\sigma \in S_n$. Then $\sigma^m = e$. Therefore $\operatorname{sgn}(\sigma^m) = \operatorname{sgn}(e)$. But sgn is a homomorphism so $\operatorname{sgn}(\sigma^m) = \operatorname{sgn}(\sigma)^m$ and $\operatorname{sgn}(e) = 1$. Therefore $\operatorname{sgn}(\sigma)^m = 1$.

But σ is an odd permutation so $\operatorname{sgn}(\sigma) = -1$. Therefore $(-1)^m = 1$, which means that m must be a multiple of 2. □

Problem 6. Let $X = \{1, 2, 3, 4, 5\}$ and let Y be the set of subsets of X.

(a) How many elements does Y have?

Solution. If we want to describe a subset of X we have to decide, for each number $1, \ldots, 5$, whether that number is in the subset. That's a sequence of 5 yes or no questions that can be answered independently for a total of $2^5 = 32$ possibilities. □

For each $\sigma \in S_5$, let $T_\sigma : Y \to Y$ be the function defined by $T_\sigma(A) = \{\sigma(x) \mid x \in A\}$.

(b) Compute $T_{(15)(234)}(\{1, 3, 4\})$.

Solution.

$$T_{(15)(234)}(\big\{1, 3, 4\big\}) = \big\{5, 4, 2\big\} = \big\{2, 4, 5\big\}.$$

□

(c) Compute $T_{(23)}(\{1, 5\})$.

Solution.
$$T_{(23)}(\{1,5\}) = \{1,5\}$$
□

(d) List the elements of the stabilizer of $\{1,2,3\}$. Recall that the stabilizer of an element $y \in Y$ is the set of all $\sigma \in S_5$ such that $T_\sigma(y) = y$.

Solution. The stabilizer consists of the elements
$$e, (123), (132), (12), (13), (23), (45), (123)(45), (132)(45), (12)(45), (13)(45), (23)(45).$$
□

(e) How many elements will there be in the orbit of $\{1,2,3\}$ under the action of S_5 on Y?

Solution. Let G be the stabilizer of $\{1,2,3\}$ and O be its orbit. Then $\#(G)\#(O) = \#(S_5)$. The size of S_5 is $5! = 120$ and we have just seen that $\#(G) = 12$ so $\#(O)$ must be 10. □

(f) (Extra credit) Prove that the stabilizer subgroup of $\{1,2,3\}$ is isomorphic to $S_3 \times S_2$. You may use the fact that $\varphi(\sigma) = T_\sigma$ is a homomorphism from S_5 into S_Y without proving it.

Solution. Instead of writing $S_3 \times S_2$, we will write $S_{\{1,2,3\}} \times S_{\{4,5\}}$. Let G be the stabilizer of $\{1,2,3\}$ in S_5. We construct a homomorphism
$$\psi : S_{\{1,2,3\}} \times S_{\{4,5\}} \to G$$
by the rule $\psi(\sigma,\tau) = \sigma\tau$. First we check that $\psi(\sigma,\tau)$ is actually in G since it is only automatic from the definition that $\psi(\sigma,\tau) \in S_5$. To check this, we have to check that $T_{\psi(\sigma,\tau)}(\{1,2,3\}) = \{1,2,3\}$. Here is the check:
$$\begin{aligned}
T_{\psi(\sigma,\tau)}(\{1,2,3\}) &= T_{\sigma\tau}(\{1,2,3\}) && \text{definition of } \psi \\
&= T_\sigma T_\tau(\{1,2,3\}) && \text{since } \varphi \text{ is a homomorphism} \\
&= T_\sigma(\{1,2,3\}) && \text{since } \tau \in S_{\{4,5\}},\ T_\tau \text{ fixed } \{1,2,3\} \\
&= \{1,2,3\} && \text{since } \sigma \in S_{\{1,2,3\}},\ T_\sigma \text{ fixes } \{1,2,3\}.
\end{aligned}$$
Now we check that ψ is a homomorphism
$$\begin{aligned}
\psi((\sigma,\tau)(\sigma',\tau')) &= \psi(\sigma\sigma',\tau\tau') && \text{definition of multiplication in } S_{\{1,2,3\}} \times S_{\{4,5\}} \\
&= \sigma\sigma'\tau\tau' && \text{definition of } \psi \\
&= \sigma\tau\sigma'\tau' && \tau \text{ and } \sigma' \text{ are disjoint so they commute} \\
&= \psi(\sigma,\tau)\psi(\sigma',\tau') && \text{definition of } \psi.
\end{aligned}$$
Note that it was very important in the above argument that σ' and τ permuted disjoint subsets of $\{1,2,3,4,5\}$. If this weren't true, we couldn't exchange their order!

Now we have to check that ψ is a bijection. Since $S_3 \times S_2$ and G both have 12 elements, it's enough to show that ψ is injective. Suppose that $\psi(\sigma,\tau) = \psi(\sigma',\tau')$. Then for any $x \in \{1,2,3,4,5\}$ we have $\psi(\sigma,\tau)(x) = \psi(\sigma',\tau')(x)$. Now, either $x \in \{1,2,3\}$ or $x \in \{4,5\}$. In the first case, we get
$$\begin{aligned}
\psi(\sigma,\tau)(x) &= \psi(\sigma',\tau')(x) \\
\sigma\tau(x) &= \sigma'\tau'(x) && \text{definition of } \psi \\
\sigma(x) &= \sigma'(x) && \text{since } x \in \{1,2,3\} \text{ and } \tau,\tau' \in S_{\{4,5\}}.
\end{aligned}$$
This holds for any $x \in \{1,2,3\}$, so $\sigma = \sigma'$. If on the other hand $x \in \{4,5\}$, we get
$$\begin{aligned}
\psi(\sigma,\tau)(x) &= \psi(\sigma',\tau')(x) \\
\sigma\tau(x) &= \sigma'\tau'(x) && \text{definition of } \psi \\
\tau(x) &= \tau'(x) && \text{since } x \in \{4,5\} \text{ and } \sigma,\sigma' \in S_{\{1,2,3\}}.
\end{aligned}$$
□

Definition 1. A **group** is a set G with an operation $* : G \times G \to G$ such that (i) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$, (ii) there is an $e \in G$ such that $e * a = a = a * e$ for all $a \in G$, and (iii) for any $a \in G$ there is an $a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$. The group G is said to be **abelian** if $a * b = b * a$ for all $a, b \in G$.

A subset $H \subset G$ is called a **subgroup** if (i) for all $a, b \in H$ the element $a * b$ is in H, and (ii) H is a group with operation $*$.

A group is called **cyclic** if it is isomorphic $\mathbf{Z}$ or it is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ for some integer n.

The **order** of an element g of a group G (written multiplicatively with identity element 1) is the smallest positive integer n such that $g^n = 1$.

Definition 2. Suppose that G and H are groups with operations written multiplicatively. A **homomorphism** $\varphi : G \to H$ is a function $\varphi : G \to H$ such that $\varphi(xy) = \varphi(x)\varphi(y)$. A homomorphism is called an **isomorphism** if it is also a bijection.

The **kernel** of φ is the set $\ker(\varphi) = \{x \in G \mid \varphi(x) = 1\}$ where 1 is the identity in H.

The **image** of φ is the set $\operatorname{im}(\varphi) = \{y \in H \mid \exists x \in G,\ y = \varphi(x)\}$.

Definition 3. An **action** of a group G on a set X is a homomorphism $\varphi : G \to S_X$. Use the notation $T_g = \varphi(g)$. The **stabilizer** of an element $x \in X$ is $\{g \in G \mid T_g(x) = x\}$. The **orbit** of $x \in X$ is $\{y \in X \mid \exists g \in G,\ T_g(x) = y\}$.

Notation

$\mathbf{Z}$ is the set of integers and $\mathbf{R}$ is the set of real numbers.

D_n is the set of rigid symmetries of a regular n-gon.

$\mathbf{Z}/n\mathbf{Z}$ is the set of equivalence classes of integers modulo n.

$\gcd\{a_1, \ldots, a_n\}$ denotes the greatest common divisor of integers $a_1, \ldots, a_n$.

If X is a set, S_X is the set of bijections from X to itself. If $X = \{1, 2, \ldots, n\}$ then S_X is also written S_n.

If $\sigma \in S_n$ the sign of σ is the expression $\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{x_{\sigma(i)} - x_{\sigma(j)}}{x_i - x_j}$. An element of S_n is called a **transposition** if it exchanges two numbers and leaves all others unchanged. An element of S_n is called **even** if its sign is 1 and **odd** if its sign is -1. The set of even elements of S_n is denoted A_n.

Theorems

Proposition 1. *The following are abelian groups: (i) $\mathbf{Z}$ under addition, (ii) $\mathbf{Z}/n\mathbf{Z}$ under addition, (iii) $\mathbf{R}$ under addition, (iv) $\mathbf{R}^*$ under multiplication, (v) $\mathbf{C}^*$ under multiplication, (vi) S_X if X is a set with 2 or fewer elements.*

The following are non-abelian groups: (vii) D_n, (viii) S_X if X is a set with 3 or more elements.

Theorem 2 (Cayley's theorem)**.** *Every group is isomorphic to a subgroup of the group of symmetries of some set.*

Proposition 3. *Let G be a group. A subset $H \subset G$ is a subgroup if and only if both (i) $H \neq \varnothing$, and (ii) for all $a, b \in H$ the element ab^{-1} is in H.*

Theorem 4. *If x and y are integers with greatest common divisor d there are integers a and b such that $ax + by = d$.*

Theorem 5. *If G is a cyclic group then every subgroup of G is cyclic.*

Proposition 6. *Suppose that G and H are groups with operations written multiplicatively and identity elements both called 1. If $\varphi : G \to H$ is a homomorphism of groups then (i) $\varphi(1) = 1$, (ii) $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in G$, (iii) $\ker(\varphi)$ is a subgroup of G, (iv) $\operatorname{im}(\varphi)$ is a subgroup of H.*

Proposition 7. *If $\sigma \in S_n$ then $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ and the function $\operatorname{sgn} : S_n \to \{\pm 1\}$ is a homomorphism. If τ is a transposition then $\operatorname{sgn}(\tau) = -1$.*

Proposition 8. *For complex numbers z and w, we have $|zw| = |z|\,|w|$.*

Proposition 9. *If $\varphi : G \to H$ is an isomorphism of groups then $\varphi^{-1} : H \to G$ is also an isomorphism.*

Proposition 10. *The inverse of a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by $\frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ provided $\frac{1}{ad - bc}$ exists.*

Proposition 11. *Let g be an element of a group G and suppose $g^n = 1$. Then $\operatorname{ord}(g)$ is finite and divides n.*

Theorem 12. *Let $\varphi : G \to S_X$ be a group action. For $x \in X$, let G_x be the stabilizer of x and let O_x be the orbit of x. If G is finite then $\#G_x \cdot \#O_x = \#G$.*