Homework 8

Submission Instructions: You are responsible to read these instructions. Failure to submit correctly as described below will result in point deductions or loss of credit for entire problems. Submit these problems on Gradescope by Sunday, March 24th, at 11:59pm. Each problem should be on a separate page (or pages). **You will need to scan a PDF of the assignment AND select the pages belonging to each problem when you submit on gradescope.**

1. An isomorphism from a group G to itself is called an *automorphism*. Let $\mathrm{Aut}(G)$ denote the set of automorphisms of a group G.
   (a) Let $f\colon G_1 \to G_2$ and $g\colon G_2 \to G_3$ be group homomorphisms. Prove that the composition $g \circ f\colon G_1 \to G_3$ is a group homomorphism.
   (b) Let $f\colon G \to H$ be a group isomorphism. Prove that the inverse function $f^{-1}\colon H \to G$ is also a group isomorphism.
   (c) Prove that $\mathrm{Aut}(G)$ is a group with operation given by composition.
   (d) Prove that $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.
   (e) Prove that $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

(a) For $x, y \in G_1$, we have

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y).$$

(b) Let $x, y \in H$. We must show that $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. Since f and f^{-1} are inverse functions, this is equivalent to checking $f(f^{-1}(xy)) = f(f^{-1}(x)f^{-1}(y))$. The left side is xy, and since f is a homomorphism the right side is $f(f^{-1}(x))f(f^{-1}(y)) = xy$.

(c) By (1), composition gives a well-defined operation on $\mathrm{Aut}(G)$ (because the composition of two bijections is a bijection). This operation is associative because composition of functions is associative. The automorphism $e : G \to G$ given by $e(g) = g$ is an identity for the composition operation. By (2) inverses exist for the operation.

(d) For $n \in \mathbb{Z}$, let $\alpha_n\colon \mathbb{Z} \to \mathbb{Z}$ be the group homomorphism given by $\alpha_n(z) = nz$. If $\alpha\colon \mathbb{Z} \to \mathbb{Z}$ is any homomorphism, then setting $n = \alpha(1)$ we have $\alpha = \alpha_n$; indeed, for $z \geq 0$ we have $\alpha(z) = nz$ by the additivity property of a group homomorphism, and for $z < 0$ we can use $\alpha(z) = -\alpha(-z)$ to conclude $\alpha(z) = nz$.
Clearly, α_n is an automorphism if and only if $n = \pm 1$, so $\mathrm{Aut}(\mathbb{Z}) = \{\alpha_1, \alpha_{-1}\}$. Note that α_1 is the identity of the group $\mathrm{Aut}(\mathbb{Z})$ and $\alpha_1 \circ \alpha_{-1} = \alpha_{-1} \circ \alpha_1 = \alpha_{-1}$ and $\alpha_{-1} \circ \alpha_{-1} = \alpha_1$. Therefore, the map $\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z})$ sending $0 \mapsto \alpha_1$ and $1 \mapsto \alpha_{-1}$ is an isomorphism.

(e) To see that $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$, we start by observing that any automorphism α of $\mathbb{Z}_2 \times \mathbb{Z}_2$ must have $\alpha((0,0)) = (0,0)$, and is a bijection of the remaining elments

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{(0,0)\} = \{s_1 = (1,0), s_2 = (1,1), s_3 = (0,1)\}.$$

Therefore, α corresponds to a permutation of $\{1,2,3\}$ via

$$\alpha(s_1) = s_i \quad \alpha(s_2) = s_j \quad \alpha(s_3) = s_k \quad \rightsquigarrow \quad \begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$$

One can then check by brute force that every permutation gives a group homomorphism.

I'll give two other proofs which may come up, and also to give additional insight.

(1) One might realize that $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) = \mathrm{GL}_2(\mathbb{Z}_2)$, and compute that there are 6 elements in $\mathrm{GL}_2(\mathbb{Z}_2)$: indeed, for any 2×2 matrix with $\mathbb{Z}_2$ entries to be invertible, we can choose any nonzero vector for the first row, for which there are 3 choices (any nonzero element of $\mathbb{Z}_2 \times \mathbb{Z}_2$). For the second row, we just need a vector that is not in the span of the first, for which there are 2 other choices. Thus, $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathrm{GL}_2(\mathbb{Z}_2)$ is a non-abelian group of order 6. Some cleverness will prove that there is only one non-abelian group of order 6 up to isomorphism, which is S_3; for example, one might follow the ideas in Adventure Sheet 15.D, writing down a multiplication table.

(2) One might realize that for any enumeration

$$(\mathbb{Z}_2 \times \mathbb{Z}_2) = \{(0,0), s_1, s_2, s_3\}$$

we have $s_i + s_j = s_k$, so any $\alpha \in \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ is determined by choosing $\alpha(s_1)$ and $\alpha(s_2)$. These must be distinct elements, but otherwise any choices work. Therefore, we have $\binom{3}{2} = 6$ automorphisms. Again, some cleverness/brute force will prove that any group of order 6 that isn't abelian must be isomorphic to S_3.

2. Let G be a group. The **center** of G is the set $Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$.
   1. Prove that $Z(G)$ is an abelian subgroup of G.
   2. Compute the center of D_4.
   3. Compute the center of S_3.
   4. Compute the center of $GL_2(\mathbb{R})$.

(a) This is almost Theorem 7.13 in the book. See the proof there that $Z(G)$ is a subgroup. To see it is abelian, take any two elements $g_1, g_2 \in Z(G)$. We need to check that $g_1 g_2 = g_2 g_1$, but this is clear since $g_1 \in Z(G)$.

(b) Looking at the table for D_4, we see that only e and r_2, rotation through 180°, commute with every other element of D_4. So the center of D_4 is $\{e, r_2\}$.

(c) No 2-cycle is in the center: $(i\,j)(j\ k) = (i\,j\,k) \neq (i\,k\,j) = (j\ k)(i\,j)$. No three cycle is in the center: $(i\,j\ k)(k\ l) = (i\,j\ k\ l) \neq (i\ j\ l\ k) = (k\ l)(i\,j\ k)$ Since e is the only element of S_3 that is not a 2-cycle or 3-cycle, the center is $\{e\}$.

(d) The center of $GL_2(\mathbb{R})$ is the subgoup of constant matrices: $\{\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix} \mid \lambda \in \mathbb{R}^\times\}$. We know from Math 217 that constant matrices commute with every matrix, so the constant matrices are in the center. For the other direction, suppose that $A = \begin{bmatrix}a & b\\ c & d\end{bmatrix}$ is in the center. Let $E_1 = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$. Since $E_1 \in GL_2$, A must commute with E_1,

which say that $AE_1 = E_1A$, or $\begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$. This tells us $a = d$ and $b = c$, so we can assume $A = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$. But also $E_2 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \in GL_2$, so $AE_2 = E_2A$, or $\begin{bmatrix} -a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} -a & -b \\ b & a \end{bmatrix}$. This tells us $b = -b$, so $b = 0$. So $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

3. Consider the symmetric group S_n, with $n \geq 3$. The goal of this problem is to prove that S_n can be generated by only two elements.
   (a) Let $\tau \in S_n$ be a permutation, and $(\,a\,b\,)$ be a transposition. Show that $\tau(\,a\,b\,)\tau^{-1} = (\,\tau(a)\,\tau(b)\,)$, the transposition changing $\tau(a)$ and $\tau(b)$.
   (b) Show that $(\,i\,j\,) = (\,1\,i\,)(\,1\,j\,)(\,1\,i\,)$. Conclude that every element of S_n is the product of transpositions of the form $(\,1\,i\,)$.
   (c) Let σ be the $(n-1)$-cycle $(\,2\,3\,\cdots\,n\,)$. Show that $(\,1\,i\,) = \sigma^{i-2}(\,1\,2\,)(\sigma^{-1})^{i-2}$ for all $i = 2, \ldots, n$. Conclude that $S_n = \langle(\,1\,2\,), (\,2\,3\,\cdots\,n\,)\rangle$.

Important note: a permutation is a FUNCTION $\{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$.

(a) Write $\sigma = \tau(\,a\,b\,)\tau^{-1}$. Then

$$\sigma(\tau(a)) = \left(\tau(a\,b)\tau^{-1}\right)(\tau(a)) = (\tau(a\,b))\,(a) = \tau(b).$$

Similarly, we can show that $\sigma(\tau(b)) = \tau(a)$. Moreover, given $k \neq \tau(a), \tau(b)$, we have $\tau^{-1}(k) \neq a, b$. Therefore,

$$\sigma(k) = \left(\tau(a\,b)\tau^{-1}\right)(k) = (\tau(a\,b))\,(\tau^{-1}(k)) = \tau(\tau^{-1}(k)) = k.$$

We conclude that σ switches $\tau(a), \tau(b)$ and fixes all other elements.

(b) For the notation $(i\,j)$ to make sense, we are implicitly assuming that $i \neq j$. Similarly, for $(1\,i)$ and $(1\,j)$ to make sense, we are implicitly assuming that $i \neq 1$ and $j \neq 1$. Apply the previous formula with $\tau = (1\,i)$, $a = 1$, and $b = j$ (note that τ is its own inverse). Then $(\,1\,i\,)(\,1\,j\,)(\,1\,i\,) = (\,i\,j\,)$ follows immediately, because $\tau(1) = i$ and $\tau(j) = j$. Since every element in S_n is a product of transpositions (Theorem 7.26) and any transposition is a product of elements of the form $(1\,i)$, we conclude that every element is a product of transpositions of the form $(1\,i)$.

(c) First, note that $(\sigma^{-1})^{i-2} = \left(\sigma^{i-2}\right)^{-1}$. Therefore,

$$\sigma^{i-2}(\,1\,2\,)(\sigma^{-1})^{i-2} = \left(\sigma^{i-2}(1)\ \sigma^{i-2}(2)\right) = (1\ \ i).$$

Indeed, since 1 doesn't appear in the cycle expression of σ, then $\sigma(1) = 1$, so $\sigma^{i-2}(1) = 1$. On the other hand, $\sigma(k) = k+1$ for all $k = 2, \ldots, n-1$. Hence $\sigma^{i-2}(2) = \sigma^{i-3}(3) = \ldots = \sigma(i-1) = i$ for all $i = 2, \ldots, n$.

In particular, $\langle(\,1\,2\,), (\,2\,\cdots\,n\,)\rangle$ contains all the transpositions of the form $(1\,i)$, and by part (c), all elements of S_n.

4. Consider the alternating group A_n, that is, the subgroup of S_n consisting of all the even permutations of S_n, for $n \geq 3$. Let $i, j, k, l \in \{1, 2, \ldots, n\}$, with $i \neq j$ and $k \neq l$.

   (a) Suppose that $(i\,j)$ and $(k\,l)$ are not disjoint cycles. Show that $(i\,j)(k\,l)$ is either the identity or a 3-cycle.

   (b) Suppose that $(i\,j)$ and $(k\,l)$ are disjoint cycles. Show that $(i\,j)(k\,l)$ is the product of two 3-cycles.

   (c) Prove that A_n is generated by the set of all 3-cycles of S_n.

(a) Since $(a\,b) = (b\,a)$, we can assume without loss of generality that $j = k$.
If $i = l$, then $(i\,j)(k\,l) = (i\,j)(j\,i) = e$, where e is the identity.
If $i \neq l$, then $(i\,j)(k\,l) = (i\,j)(j\,l) = (i\,j\,l)$ (see Theorem 7.26 for the last equality), which is a 3-cycle.

(b) Since $(j\,k)$ has order 2, we have that $(i\,j)(k\,l) = (i\,j)(j\,k)(j\,k)(k\,l)$. By part (a), $(i\,j)(j\,k) = (i, j, k)$ and $(j\,k)(k\,l) = (j, k, l)$, two 3-cycles, which concludes the proof.

(c) Every element of A_n can be written as a product of an even number of transpositions. Let $\sigma \in A_n$. There exists k a positive integer such that σ is the product of $2k$ transpositions. Equivalently, σ is the product of k elements $\tau_1 \ldots \tau_k$, where τ_i is a product of two transpositions for all $i = 1, \ldots, k$. Hence, by parts (a) and (b), τ_i is in the subgroup generated by the set of all 3-cycles of S_n, so σ is in the subgroup generated by the set of all 3-cycles of S_n. Hence, we have proved that A_n is contained in the subgroup of S_n generated by the set of all 3-cycles of S_n. The other containment follows from the last line of our solution to part (a), which in particular tells us that 3-cycles are even permutations.