You may submit your solutions via assignment page on the canvas website of the course.

For collaboration and late days policy, see course website at http://madhu.seas.harvard.edu/courses/Fall2016

Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.

Problems marked [AM106] or [AM106-X] are for AM106 students (though AM206 students should confirm that they know how to do them), and those marked [AM206-X] are for AM206 students. (Problems with no labels should be answered by all students.) However, AM106 students can do a problem marked [AM206-X] instead of one marked [AM106-X] (for the same value of X) if they wish (out of interest, or for a challenge). If you wish to keep the option of staying in either AM106 or AM206 open until add/drop date, then you should do all problems marked [AM106] and all problems marked [AM206-X].

Problem 1. (Orders of Permutations) What are all the possible orders for elements of $S_8$ and of $A_8$? Justify your answers.

Solution. $S_8$ has elements of order 1 to 8 (the identity and cycles of length 2 to 8 give these), of order 10 (the permutation (12)(34567)), 12 (the permutation (123)(4567)) and 15 (the permutation (123)(45678)), and these are the only orders. To see the latter note that any permutation is given by the length of its cycles $\ell_1, \ldots, \ell_k$ where $\ell_i \geq 1$ and $\sum \ell_i = 8$, and the order of the permutation is $\text{lcm}(\ell_1, \ldots, \ell_k)$. The above numbers are the only ones satisfying this condition. In particular the only multiple of 7 admissible is 7 itself. The only multiples of 5 are 5, 10 and 15. Etc.

Turning to $A_8$, the orders will be a subset of the orders of $S_8$. 1, 3, 5, 7 and 15 remain admissible, since the cycles (and the two cycle) are all of odd length. 2, 4 and 6 are also admissible orders of elements of $A_8$, with element (12)(34), (123)(56) and (123456)(78) being examples of this length. 8, 10 and 12 are not admissible since they can not be generated by permutations with an even number of even cycles. (In this case the characterization of admissible orders is that the order should expressible as $\text{lcm}(\ell_1, \ldots, \ell_k)$ with $\sum \ell_i = 8$ and an even number of the $\ell_i$’s are even.)

Common Errors. TBD

Problem 2. (Generating $S_n$) For a group $G$ and elements $g_1, \ldots, g_n \in G$, the subgroup generated by $g_1, \ldots, g_n$ is defined to be the set of all elements we can obtain by multiplying the $g_i$’s and their inverses together any number of times. Formally:

$$\langle g_1, \ldots, g_n \rangle = \left\{ g_{i_1}^{k_1} g_{i_2}^{k_2} \cdots g_{i_t}^{k_t} : t \in \mathbb{N}, i_1, \ldots, i_t \in \{1, \ldots, n\}, k_1, \ldots, k_t \in \mathbb{Z} \right\}.$$
(Note that a *cyclic* subgroup is a subgroup generated by a *single* generator $g$. Here we allow multiple generators, so these subgroups need not be cyclic.)

Prove that for $n \geq 2$, $S_n = \langle (12), (12\cdots n) \rangle$. (Hint: repeatedly use conjugation to obtain all the transpositions.)

**Solution.** We first note that every tranposition $(i, i+1)$ can be generated from $(12)$ and $(12\cdots n)$. This is so since $(i, i+1) = (12\cdots n)^{-1}(12)(12\cdots n)^{(i-1)}$.

Next note that any transposition $(i, j)$ can be generated from the above. To see this assume w.l.o.g. that $i < j$. Then we have $(i, j) = (j-1, j) \cdots (i+1, i+2)(i, i+1)(i+1, i+2) \cdots (j-1, j)$.

Next we can generate any cycle $(i_1i_2\cdots i_m)$ since it equals $(i_1i_2)(i_2i_3)\cdots(i_{m-1}i_m)$.

Lastly we know that any permutation can be expressed as a product of cycles. We conclude that any permutation can be generated from $(12)$ and $(12\cdots n)$.

**Common Errors.** TBD

**Problem 3. (Isomorphisms of Specific Groups)** For each of the following pairs of groups $(G, H)$, determine whether or not they are isomorphic. If not, determine whether one is isomorphic to a subgroup of the other. Justify your answers.

1. [AM106-A] $\mathbb{Z}_5$ vs. $S_5$.
2. $\mathbb{Z}_8^*$ vs. $\mathbb{Z}_{12}^*$.
3. $\mathbb{R}^*$ vs. $\mathbb{C}^*$.
4. [AM206-A] $\mathbb{R}$ vs. $GL_2(\mathbb{R})$.

**Solution.**

1. $\mathbb{Z}_5$ is not isomorphic to $S_5$, since the former has order 5 while the latter has order 120. But $\mathbb{Z}_5 \cong \langle (12345) \rangle \leq S_5$.

2. $\mathbb{Z}_8^*$ is isomorphic to $\mathbb{Z}_{12}^*$. The elements of $\mathbb{Z}_8^*$ are $\{1, 3, 5, 7\}$ and the elements of $\mathbb{Z}_{12}^*$ are $\{1, 5, 7, 11\}$. Every bijection from $\mathbb{Z}_8^*$ to $\mathbb{Z}_{12}^*$ that maps 1 to 1 is an isomorphism! All that matters is that $\phi(i \cdot j) \not\in \{\phi(i), \phi(j)\}$ if $i \neq j$ since $i \cdot j \not\in \{i, j\}$ if $i \neq j$. So one can take, e.g., $\phi(1) = 1$, $\phi(3) = 5$, $\phi(5) = 7$ and $\phi(7) = 11$.

3. $\mathbb{R}^*$ is not isomorphic to $\mathbb{C}^*$. If it exists, such an isomorphism should send 1 (as a complex number) to 1 (as a real). Then it should map $-1$ to $-1$ so as to satisfy $\phi((-1) \cdot (-1)) = \phi(-1) \cdot \phi(-1)$. But then it will need to send $\phi(i)$ (the square root of $-1$) to a square root of $-1$ which does not exist over the reals.

4. [AM206-A] $\mathbb{R}$ is not isomorphic to $GL_2(\mathbb{R})$. In fact $\mathbb{R}$ is not even isomorphic to $\mathbb{R}^*$ which is (isomorphic to) a subgroup of $GL_2(\mathbb{R})$. An isomorphism would imply halving in $\mathbb{R}$ is equivalent to taking square-roots, but elements sometimes do not have square roots in $\mathbb{R}^*$ and others have two (both of which do not look like halving). Building on this, here’s a concrete counterexample.

Suppose $\phi: \mathbb{R} \to GL_2(\mathbb{R})$ is a bijection. Let $A$ be the matrix:

$$
\begin{bmatrix}
-1 & 0 \\
0 & 0
\end{bmatrix}.
$$
Let $\alpha = \phi^{-1}(A)$ and let $\beta = \alpha/2$ so that $\beta + \beta = \alpha$. Finally let $B = \phi(\beta)$. By the properties of the isomorphism we have $B \cdot B = \phi(\beta) \cdot \phi(\beta) = \phi(\beta + \beta) = \phi(\alpha) = A$. But there can be no such matrix (corresponding to the square root of $-1$). Formal argument below.

Suppose $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ so that $B^2 = \begin{bmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{bmatrix}$.

Since $a^2 + bc = -1$ and $d^2 + bc = 0$, we have $a^2 \neq d^2$ and so $a \neq -d$. Now since $ab + bd = ac + cd = 0$, we have $b = c = 0$. But then we conclude $a^2 + bc = a^2 = -1$ which contradicts the fact that $-1$ does not have a square root over the reals.

Common Errors. TBD

Problem 4. (From Cayley to Lagrange, Gallian 6.46)

1. Recall that in the proof of Cayley’s Theorem, the isomorphism from a group $G$ to a subgroup of $\text{Sym}(G)$ takes an element $g \in G$ to the permutation $T_g(x) = gx$. Show that for finite $G$, the disjoint cycle notation for $T_g$ consists entirely of cycles of length equal to the order of $g$.

2. Deduce the following corollary of Lagrange’s Theorem: the order of an element $g \in G$ divides the order of the group $G$.

Solution.

1. Consider the cycle containing the identity element $e$ in the permutation $T_g$. This cycle has the form $(e, g, g^2, \ldots, g^{k-1})$ for some $k$, for which we have $g^k = e$. Now consider some element $a$ not in the cycle above. Its cycle has the form $(a, a \cdot g, \ldots, a \cdot g^{\ell-1})$ for some integer $\ell$ for which we have $a \cdot g^{\ell} = a$. Left multiplying both sides by $a^{-1}$ we have $g^{\ell} = e$. By the distinctness of $\{e, \ldots, g^{k-1}\}$ and $\{a, \ldots, ag^{\ell-1}\}$ we also have that $k$ and $\ell$ are both the smallest positive integers such that $g^\ell = g^k = e$. It follows $k = \ell$ and so the cycles of $T_g$ all have the same length.

2. Since $T_g$ is a union of cycles, all of length $k$, and the cycles sum to length $n = \text{order}(G)$, it follows that $k$ must divide $n$.

Common Errors. TBD