MATH 436: Homework III.
Due in class on Friday, Oct 3

1. Let $G$ be any group. Show that the subgroup of inner automorphisms, $Inn(G)$ is normal in $Aut(G)$.

2. **[Automorphisms of $\mathbb{Z}/d\mathbb{Z}$].** For $\bar{j} \in \mathbb{Z}/d\mathbb{Z}$, define $f_j : \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ via $f_j(\bar{n}) = \bar{jn}$ for all $\bar{n} \in \mathbb{Z}/d\mathbb{Z}$. Here $\bar{n}$ denotes the class of the integer $n$ in $\mathbb{Z}/d\mathbb{Z}$.
   (a) Check that $f_j$ is a well-defined endomorphism of $(\mathbb{Z}/d\mathbb{Z}, +)$ and that $\theta : \mathbb{Z}/d\mathbb{Z} \to End((\mathbb{Z}/d\mathbb{Z}, +))$ defined by $\theta(\bar{j}) = f_j$ induces an isomorphism of the monoid $End((\mathbb{Z}/d\mathbb{Z}, +))$ with $(\mathbb{Z}/d\mathbb{Z}, \cdot)$ i.e., $\mathbb{Z}/d\mathbb{Z}$ under multiplication.
   (b) Show that $Aut((\mathbb{Z}/d\mathbb{Z}, +)) = \{ f_m | 1 \leq m < d, gcd(d, m) = 1 \}$ and that $Aut((\mathbb{Z}/d\mathbb{Z}, +)) \cong (\mathbb{Z}/d\mathbb{Z})^*$. Thus $|Aut((\mathbb{Z}/d\mathbb{Z}, +))| = \phi(d)$ where $\phi$ is Euler’s Phi function.

3. **Torsion in groups.** In any group $G$, an element $x$ is called a torsion element if it has finite order, i.e., $x^k = e$ for some integer $k \geq 1$. A group where all elements have finite order is called a torsion group. A group where all non-identity elements have infinite order is called torsion-free. Let $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ denote respectively the groups of integers, rationals and real numbers under addition.
   (a) Show that $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{R}/\mathbb{Q}$ are torsion-free groups.
   (b) Show that $\mathbb{Q}/\mathbb{Z}$ is an infinite torsion group.
   (c) Let $G$ be a group and let $x, y$ be torsion elements with $o(x) = m$ and $o(y) = n$. Show that if $xy = yx$ then $o(xy)$ divides $lcm(m, n)$ where $lcm$ stands for least common multiple. If $gcd(m, n) = 1$ show that $o(xy) = mn$. Conclude that in an Abelian group $A$, the set of torsion elements $A_{tor}$ forms a normal subgroup. Show that $A/A_{tor}$ is torsion-free.
   (d) Consider the matrices $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Show that they are in the special linear group $SL_2(\mathbb{R})$. Find the orders of $A, B$ and $AB$. Do the results in (c) apply here? Do the set of torsion elements in $SL_2(\mathbb{R})$ form a subgroup of $SL_2(\mathbb{R})$?
   (e) Let $S^1 = \{ z \in \mathbb{C} | |z| = 1 \}$ be the set of complex numbers of unit length. Show that $S^1$ is a group under multiplication and construct an isomorphism between it and $(\mathbb{R}/\mathbb{Z}, +)$. $S^1$ is called the unit circle group.

4. **Order of elements in $\Sigma_n$.** For $\sigma \in \Sigma_n$ we define the support of $\sigma$, denoted $Supp(\sigma)$ by $Supp(\sigma) = \{ j | 1 \leq j \leq n, \sigma(j) \neq j \}$. Thus on
{1, \ldots, n} - \text{Supp}(\sigma), \sigma \text{ acts like the identity map.}
(a) Show that if \text{Supp}(\sigma) \cap \text{Supp}(\mu) = \emptyset \text{ then } \sigma \circ \mu = \mu \circ \sigma \text{ in } \Sigma_n.
(b) \sigma \in \Sigma_n \text{ is called a cycle if in the cycle notation it is represented as a single cycle } (a_1, \ldots, a_k). \text{ For example } (12) \text{ and } (134) \text{ are cycles in } \Sigma_4 \text{ whereas } (12)(34) \text{ is not. Show that if } \sigma = (a_1, \ldots, a_k) \text{ then } \sigma \text{ has order } k \text{ in } \Sigma_n.
(c) Now take } \mu \in \Sigma_n, \text{ we have seen that we may write } \mu \text{ as a product of disjoint cycles. What is the order of } (12)(34)(567) \subseteq \Sigma_7? \text{ What is the order of a general element } \mu \in \Sigma_n \text{ if } \mu \text{ can be written as a product of disjoint cycles of (not necessarily distinct) lengths } m_1, \ldots, m_s.

5. \textbf{Minimal sets of generators.} \text{Let } \{s_1, \ldots, s_d\} \text{ be a minimal set of generators for } G. \text{ ("Minimal" means no smaller set generates } G. \text{ By convention we say that the emptyset generates the trivial group } \{e\}. ) \text{ Consider the set }

T = \{s_1^{\delta_1} \cdots s_d^{\delta_d} | \delta_j = 0, 1 \text{ for all } 1 \leq j \leq d\}.

\text{Show that } |T| = 2^d \text{ (Be careful here! You need to show there are no repeats in the list of elements in the definition of } T. ) \text{ and conclude that } d \leq \log_2(|G|). \text{ Here } \log_2 \text{ is defined via } 2^{\log_2(a)} = a \text{ for all real } a > 0. \text{ Thus any group } G \text{ can be generated by less than or equal to } \log_2(|G|) \text{ generators.}

6. \textbf{Conjugation and normalcy in } \Sigma_n.
(a) Show that \Sigma_n \text{ is generated by the } n - 1 \text{ transpositions }

\{(12), (13), (14), \ldots, (1n)\}.

[Hint: Compute (1i)(1j)(1i). Also recall that Lang proves that the set of all transpositions generates } \Sigma_n \text{ on Page 13.]
(b) Show that \Sigma_n \text{ is generated by the } n - 1 \text{ transpositions }

\{(12), (23), (34), (45), \ldots, (n - 1n)\}.

[Hint: Compute (1, j - 1)(j - 1, j)(1, j - 1).]

7. \textbf{Some generating sets for } \Sigma_n.
(a) Show that if } \sigma = (i_1, i_2, \ldots, i_k) \text{ is a cycle in } \Sigma_n \text{ and } \tau \in \Sigma_n \text{ then } \tau \sigma \tau^{-1} \text{ is a cycle of the form } (\tau(i_1), \ldots, \tau(i_k)).
(b) Let } \alpha = (12)(346) \text{ and } \tau = (354)(21) \in \Sigma_6. \text{ Explain how to use (a) to calculate } \tau \alpha \tau^{-1}.
(c) Let } K = \{e, (12)(34), (13)(24), (14)(23)\} \subset \Sigma_4. \text{ Show that } K \text{ is a normal
subgroup of \( \Sigma_4 \) and that \( K \) is Abelian but not cyclic. \( K \) is called the Klein four subgroup of \( \Sigma_4 \). Show that \( N = \{e, (12)(34)\} \) is a normal subgroup of \( K \) but not a normal subgroup of \( \Sigma_4 \). Thus \( N \) is normal in \( K \), \( K \) is normal in \( \Sigma_4 \) but \( N \) is not normal in \( \Sigma_4 \). Hence the relation of being a normal subgroup is not transitive.

8. **Metrics and Volumes for Groups.** Recall a metric on a set \( X \) is a function \( d: X \times X \to \mathbb{R} \) such that

(i) \( d(x, y) \geq 0 \) and \( d(x, y) = 0 \) if and only if \( x = y \).
(ii) \( d(x, y) = d(y, x) \) for all \( x, y \in X \).
(iii) \( d(x, z) \leq d(x, y) + d(y, z) \) for all \( x, y, z \in X \).

(a) Let \( G \) be a group with generating set \( S \). We define

\[
d_S(x, y) = \min\{k | k \in \mathbb{N}, x s_1^{\pm 1} \ldots s_k^{\pm 1} = y, s_j \in S\}.
\]

Show that \( d_S \) is a metric on \( G \). It is called the Cayley metric on \( G \) with respect to the generating set \( S \).

(b) If \( G \) is a finitely generated group with two different finite generating sets \( S \) and \( T \), show that \( d_S \) and \( d_T \) are equivalent, i.e., there are real numbers \( c, C > 0 \) such that \( c d_T(x, y) \leq d_S(x, y) \leq C d_T(x, y) \) for all \( x, y \in G \). Thus Cayley metrics coming from different finite generating sets for the same finitely generated group are equivalent metrics.

(c) Let \( G \) be a group with finite generating set \( S \). We define the volume function \( V_S: \mathbb{N} \to \mathbb{N} \) by \( V_S(n) = |\{g \in G|d_S(g, e) \leq n\}| \). Thus \( V_S(n) \) counts the number of elements whose distance from \( e \) does not exceed \( n \) in the Cayley metric. Show that \( V_S(n) \leq (2|S| + 1)^n \) for all \( n \in \mathbb{N} \).

(d) Let \( \mathbb{Z} \times \mathbb{Z} = \{(a, b) | a, b \in \mathbb{Z}\} \). This is a subgroup of \( \mathbb{R}^2 \) under addition. It is easy to check that \( S = \{(0, 1), (1, 0)\} \) is a generating set for \( \mathbb{Z} \times \mathbb{Z} \). Show that \( d_S((m_1, m_2), (n_1, n_2)) = |m_1 - n_1| + |m_2 - n_2| \) and \( V_S(n) = n^2 + (n + 1)^2 \) in this example.