MATH 436: Homework IV.
Due in class on Friday, Oct 10

1. Let G be a finite group and let p be the smallest prime that divides $|G|$. Show that if $A \trianglelefteq G$ has $|A| = p$, then $A \leq Z(G)$, where $Z(G)$ is the center of G.

2. [**Semidirect Products**] Recall that for K, H groups and $\phi : H \to Aut(K)$ a homomorphism we define the semi-direct product of H and K via ϕ as $G = K \rtimes_\phi H$.
As a set $G = K \times H$ but the binary operation $\star : G \times G \to G$ is given by

$$(k_1, h_1) \star (k_2, h_2) = (k_1 k_2^{\phi(h_1)}, h_1 h_2)$$

where we have used the notation $k_2^{\phi(h_1)}$ for $\phi(h_1)(k_2) \in K$.

In class we showed that $e = (e_K, e_H)$ is a two-sided identity for this binary operation. Here e_K and e_H are the identity elements of K and H respectively.
(a) Show that the binary operation $\star$ is associative.
(b) Show that $((k^{-1})^{\phi(h^{-1})}, h^{-1})$ is a two-sided inverse for (k, h) under this binary operation. This together with (a) then shows that G is actually a group.
(c) In class we showed that $K \overset{\lambda}{\hookrightarrow} G$ given by $\lambda(k) = (k, e_H)$ is a monomorphism. Identifying K with its image in G, we have $K \leq G$. Show that in fact $K \trianglelefteq G$.
(With this we have completed all the facts that were stated but were not proved in class.)
(d) Now assume $f : H \to \hat{H}$, $g : K \to \hat{K}$ are isomorphisms. Define $\hat{\phi} : \hat{H} \to Aut(\hat{K})$ by $\hat{\phi}(\hat{h}) = g \circ \phi(f^{-1}(\hat{h})) \circ g^{-1}$ for all $\hat{h} \in \hat{H}$. Check that $\hat{\phi}$ is a well-defined homomorphism between the stated domain and codomain. Then check that the map $\Theta : K \rtimes_\phi H \to \hat{K} \rtimes_{\hat{\phi}} \hat{H}$ given by $\Theta((k, h)) = (g(k), f(h))$ is an isomorphism of the two semi-direct products.
(e) Given H, K and two homomorphisms $\phi, \psi : H \to Aut(K)$. Show that if there is $g \in Aut(K)$ such that $\psi(h) = g \circ \phi(h) \circ g^{-1}$ for all $h \in H$, then $K \rtimes_\psi H$ is isomorphic to $K \rtimes_\phi H$. In this case we call ψ and ϕ conjugate gluing maps, thus conjugate gluing maps give isomorphic semi-direct products.

3. [**Jordan's Theorem**] Let G be a finite group.
(a) If H is a proper subgroup of G, i.e., $H \neq G$, show that $G \neq \bigcup_{g \in G} gHg^{-1}$.

[Hint: Count the number of elements in the union carefully.]
(b) Suppose G acts transitively on X and $|X| \geq 2$. Show that there exists $g \in G$ such that $g \cdot x \neq x$ for all $x \in X$.

4. **[Burnside's Lemma]** A subset C of $X \times Y$ is called a correspondence between X and Y.
(a) Let $C \subset X \times Y$ be a correspondence and suppose $|X|, |Y| < \infty$. Define $\phi : X \to \mathbb{N}$ by $\phi(x) = |\{y \in Y | (x, y) \in C\}|$ and $\psi : Y \to \mathbb{N}$ by $\psi(y) = |\{x \in X | (x, y) \in C\}|$. Explain why

$$\sum_{x \in X} \phi(x) = \sum_{y \in Y} \psi(y).$$

(b) If a finite group G acts on a finite set X we define $Fix : G \to \mathbb{N}$ by $Fix(g) = |\{x \in X | g \cdot x = x\}|$ for all $g \in G$. Let $X/G = \{\mathcal{O}_x | x \in X\}$ be the set of orbits of the action. If G_x stands for the isotropy group of the point x, show that:

$$\sum_{g \in G} Fix(g) = \sum_{x \in X} |G_x| = |G||X/G|.$$

(Note $|X/G|$ is the number of distinct orbits which is not in general equal to $|X|/|G|$ so be careful of this common misleading notation.)
(c) An action of G on X is called **doubly transitive** if for any $x_1 \neq x_2 \in X$ and $y_1 \neq y_2 \in X$, there is $g \in G$ such that $g \cdot x_i = y_i$ for $i = 1, 2$. Explain why every doubly transitive action is transitive if $|X| \geq 2$. From now on $|X| \geq 2$. Consider the G action on $X \times X$ by $g \cdot (x_1, x_2) = (g \cdot x_1, g \cdot x_2)$. Show that the G action on $X \times X$ has two orbits if and only if the G action on X is doubly transitive. (Hint: Consider the subsets $\Delta(X) = \{(x, x) | x \in X\}$ and $F(X, 2) = \{(x_1, x_2) | x_1, x_2 \in X, x_1 \neq x_2\}$ of $X \times X$. Sidenote: $\Delta(X)$ is called the diagonal of $X \times X$ and $F(X, 2)$ is called the 2-fold configuration set of X.)
(d) Show that for the action of a finite group G on a finite set X with $|X| \geq 2$ we have:

$$G \text{ acts transitively on } X \leftrightarrow \sum_{g \in G} Fix(g) = |G|$$

and

$$G \text{ acts doubly transitively on } X \leftrightarrow \sum_{g \in G} Fix(g)^2 = 2|G|.$$

(e) A triply transitive action of G on X is one where given two triples of distinct elements (x_1, x_2, x_3) and (y_1, y_2, y_3) there is $g \in G$ with $g \cdot x_i = y_i$ for $i = 1, 2, 3$. Find a similar formula as in (d) that characterizes triply transitive actions on finite sets X with $|X| \geq 3$.

5. [**Orthogonal Groups**] Recall the transpose of a $n \times n$ matrix $\mathbb{A}$, denoted by $\mathbb{A}^T$ is the matrix whose (i, j)-entry is the (j, i)-entry of $\mathbb{A}$.
(a) We define $O(n) = \{n \times n \text{ matrix } \mathbb{A} | \mathbb{A}^T\mathbb{A} = \mathbb{I} = \mathbb{A}\mathbb{A}^T\}$. Show that $O(n)$ is a subgroup of $GL_n(\mathbb{R})$. It is called the group of $n \times n$ orthogonal matrices.
(b) If $\hat{a}_1, \ldots, \hat{a}_n$ are the row vectors of $\mathbb{A}$. Show that $\mathbb{A}\mathbb{A}^T = \mathbb{I}$ is equivalent to $\{\hat{a}_1, \ldots, \hat{a}_n\}$ being an orthonormal set of vectors under the standard dot product of vectors. Show also that $\mathbb{A}^T\mathbb{A} = \mathbb{I}$ is equivalent to the column vectors of $\mathbb{A}$ being an orthonormal set of vectors under the standard dot product of vectors. Thus $\mathbb{A} \in O(n)$ if and only if the columns and rows of $\mathbb{A}$ form orthonormal sets.
(c) show that the determinant gives an epimorphism $det : O(n) \to \{-1, 1\}$ where $\{-1, 1\}$ is a group under the usual multiplication. Thus the kernel is a normal subgroup of index 2. It is called the Special Orthogonal Group and is denoted $SO(n)$.
(d) If $\hat{x}, \hat{y}$ denote column vectors of $\mathbb{R}^n$ then recall the dot product $< \hat{x}, \hat{y} >$ is given by matrix multiplication $\hat{x}^T\hat{y}$. Show that $< \mathbb{A}\hat{x}, \mathbb{A}\hat{y} >=< \hat{x}, \hat{y} >$ for all $\hat{x}, \hat{y} \in \mathbb{R}^n$ when $\mathbb{A}$ is an orthogonal matrix.
(e) Let $S^{n-1} = \{\hat{x} \in \mathbb{R}^n | < \hat{x}, \hat{x} >= 1\}$. This is called the unit sphere of $\mathbb{R}^n$. Show that $\mathbb{A} \cdot \hat{x} = \mathbb{A}\hat{x}$ defines a transitive action of $O(n)$ on S^{n-1}. Let $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. Compute the isotropy group of e_1 under this action and show that it is isomorphic to $O(n-1)$. Conclude that the map $f : O(n) \to S^{n-1}$ given by

$$f(\mathbb{A}) = \text{ First column of } \mathbb{A}$$

gives a bijection between $O(n)/O(n-1)$ and S^{n-1}.
(f) Show that $O(1) = \{-1, 1\}$, $SO(1) = \{1\}$, and

$$SO(2) = \{\begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix} | 0 \leq \theta < 2\pi\}.$$

Furthermore show that $SO(2)$ is an Abelian group isomorphic to $(\mathbb{R}/\mathbb{Z}, +)$.

6. [**Automorphism groups of Graphs**] A graph is an object that consists of vertices and edges. More precisely a graph $X = (V, E)$ consists of a set of vertices V and a set of edges E whose elements are subsets of V of size 2. (We picture the subset $\{v_1, v_2\}$ as an edge line joining the vertex v_1 and the vertex v_2.). Thus formally $E \subseteq \{A \in P(V) || A| = 2\}$. We say that two vertices are adjacent in a graph if they are joined by a single edge. Given a graph $X = (V, E)$, we define

$$Aut(X) = \{f \in \Sigma(V) | \{v_1, v_2\} \in E \implies \{f(v_1), f(v_2)\} \in E\}.$$

Thus $Aut(X)$ is the subset of the permutations of the vertices that take adjacent vertices in X to adjacent vertices in X.
(a) Show that for a graph $X = (V, E)$, $Aut(X)$ is a subgroup of $\Sigma(V)$.
(b) Let C_n be the graph whose vertices are $\{1, 2, \ldots, n\}$ and where $\{v, w\}$ is an edge if and only if $v \equiv w \pm 1 \mod n$. This graph C_n is a called the n-cycle graph. Draw a picture for C_5.
(c) If C_n is an n-cycle graph for $n \geq 2$ and $\tau \in Aut(C_n)$ has $\tau(1) = 1, \tau(2) = 2$ explain why $\tau = 1_V$.
(d) Define $R, T \in \Sigma_n$ as follows. Let $R = (123 \ldots n)$. Define

$$T(j) = \begin{cases} 1 \text{ if } j = 1 \\ n - j + 2 \text{ if } 1 < j \leq n. \end{cases}$$

Show that $R, T \in Aut(C_n)$ and $o(R) = n, o(T) = 2$ for $n \geq 3$.
(e) Show in fact for $n \geq 3$, any $\lambda \in Aut(C_n)$ can be written uniquely as $\lambda = R^k T^\epsilon$ for some $0 \leq k < n$ and $\epsilon = 0, 1$. Conclude that $|Aut(C_n)| = 2n$. $Aut(C_n)$ is called the Dihedral Group of order $2n$, denoted by D_{2n}. (Warning: Some authors call it D_n!). (Hint: First show $R^s\lambda \in \Sigma_n$ fixes 1 for some s.)
(f) Fix $n \geq 3$ and let R, T be as in (e). Then show if $K =< R >, H =< T >$ that $K \trianglelefteq D_{2n}$, $KH = D_{2n}$ and $K \cap H = \{e\}$. Thus conclude that D_{2n} is isomorphic to a semi-direct product $\mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$. Describe the homomorphism $\phi : \mathbb{Z}/2\mathbb{Z} \to Aut(\mathbb{Z}/n\mathbb{Z})$.