Homework Assignment 5
Due Friday, February 26

1. We begin by proving the fourth isomorphism theorem. Let $N \trianglelefteq G$ be a normal subgroup of a group G. Let $\pi : G \to G/N$ be the natural projection.

   (a) Let $H \leq G/N$. Show that the preimage $\pi^{-1}(H) = \{g \in G : \pi(g) \in H\}$ is a subgroup of G containing N.

   (b) Let $H \leq G$. Show that its image $\pi(H)$ is a subgroup of G/N.

   (c) These constructions do not give a bijection between subgroups of G and subgroups of G/N. Give an example showing why.

   (d) If we restrict our attention to certain subgroups of G we do get a bijection. Show that the constructions in parts (a) and (b) give a bijection:

   $$\left\{ \begin{array}{c} \text{Subgroups } H \leq G \\ \text{such that } N \leq H \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{c} \text{Subgroups} \\ \overline{H} \leq G/N \end{array} \right\}$$

   (e) This bijection satisfies certain properties. First let's establish some notation. Let $H, K \in G$ be two subgroups containing N, and denote the corresponding subgroups of G/N by $\overline{H}$ and $\overline{K}$. Prove the following properties.

      i. $H \leq K$ if and only if $\overline{H} \leq \overline{K}$.
      ii. $H \trianglelefteq K$ if and only if $\overline{H} \trianglelefteq \overline{K}$.
      iii. $\overline{H \cap K} = \overline{H} \cap \overline{K}$
      iv. $\overline{\langle H, K \rangle} = \langle \overline{H}, \overline{K} \rangle$.

      Hint. *You can do (iii) and (iv) directly, but if you want to be really slick use that the intersection of two subgroups is the largest subgroup contained in both, (and the dual notion for the subgroup generated by two subgroups). Notice that this means that being the intersection of two subgroups (or generated by two subgroups) is a condition on the lattice of G (or G/N). Then the result should easily follow from part (i).*

Now let's establish some properties of one more family of finite groups, diverging from D_{2n}, S_n and direct products of cyclic groups. As we start defining more exotic properties of groups we will need to expand our library of finite groups to exhibit some of these interesting properties. Let's finish by introducing finite matrix groups. We will need a definition.

Definition 1. *A field is a set F together with two commutative binary operations, $+$ and $\cdot$ (addition and multiplication), such that $(F, +)$ and $(F \backslash \{0\}, \cdot)$ are abelian groups, and such that the distributive law holds. That is, for all $a, b, c \in F$ we have:*

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

For any field we let $F^\times = F \setminus \{0\}$ be its mutliplicative group. A field F is called a finite field if $|F| < \infty$.

It turns out that vector space theory over F is pretty much identical to vector space theory over R. We can define the first matrix group we hope to study.

Definition 2. *Let F be a field. If M, N are matrices with entries in F, we can compute their product MN and the determinant $\det(M) \in F$ using the same formulas as if $F = \mathbb{R}$. Then the general linear group of degree n over F is,*

$$GL_n(F) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries in } F \text{ and } \det(A) \neq 0\}.$$

You may use the following facts without proofs (since they are a standard result of linear algebra).

Proposition 1. *The set $GL_n(F)$ can be identified with the set of linear bijections $F^n \to F^n$, and matrix multiplication corresponds to composition of functions. In particular, $GL_n(F)$ is a group under matrix multiplication.*

Proposition 2. *If $A, B \in GL_n(F)$, then $\det(AB) = \det(A)\det(B)$. In particular, $\det : GL_n(F) \to F^\times$ is a group homomorphism.*

2. It turns out that we have seen examples of finite fields already.

   (a) Let p be a prime number. Show that $\mathbb{Z}/p\mathbb{Z}$ with the operations $+$ and $\times$ is a field. This is the *finite field of order p* and will be denoted by $\mathbb{F}_p$.

   (b) Show that if n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is not a field.

3. Now let's study $GL_2(\mathbb{F}_p)$.

   (a) Prove that $|GL_2(\mathbb{F}_2)| = 6$.

   (b) Write all the elements of $GL_2(\mathbb{F}_2)$ and compute the order of each element.

   (c) Show that $GL_2(\mathbb{F}_2)$ is not abelian. (We will later see that it is isomorphic to S_3).

   (d) Generalizing part (a), show that if p is prime then
   $$|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p.$$

4. The general linear group has lots of interesting subgroups and quotients.

   (a) Show that the constant diagonal matrices are a normal subgroup of $GL_n(F)$ isomorphic to $F^\times$.

   We will often abuse notation and denote this by $F^\times \trianglelefteq GL_n(F)$. The quotient group $GL_n(F)/F^\times$ is called the *projective general linear group* and denoted $PGL_n(F)$.

   (b) The *special linear group $SL_n(F)$* is defined
   $$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1.\}$$

   Show that $SL_n(F)$ is a normal subgroup of $GL_n(F)$ and prove that
   $$GL_n(F)/SL_n(F) \cong F^\times.$$

   (c) List all the elements of $SL_2(\mathbb{F}_2)$

   (d) Compute $|SL_2(\mathbb{F}_p)|$ (*Hint*, between 3(d) and 4(b) you've already done all the work).

   (e) Let I be the identity matrix. Show that $\{\pm I\} \leq SL_n(F)$ if and only if n is even.

   (f) Use the second isomorphism theorem to construct an isomorphism:
   $$PGL_2(\mathbb{C}) \cong SL_2(\mathbb{C})/\{\pm I\}.$$

   (As a bonus, think about why this is not true for a general field. For example, it is false over $\mathbb{R}$, or over $\mathbb{F}_p$ for $p \neq 2$.)