MATH 436: Homework V.
Due in class on Wednesday, Oct 26

1. **[Groups generated by 2 involutions.]** Let $G =< a, b >$ with $o(a) = o(b) = 2$ and assume G is not cyclic. Let $\alpha = ab$.
(a) Show that $a\alpha a^{-1} = b\alpha b^{-1} = \alpha^{-1}$. Conclude that if $K =< \alpha >$ then $K \trianglelefteq G$. Show that $aK = bK$ and use this to show $|G/K| = 2$.
(b) Let $H =< a >$ show that $HK = G$, $H \cap K = \{e\}$ and conclude that $G \cong K \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$. Check that $\phi : \mathbb{Z}/2\mathbb{Z} \to Aut(K)$ is given by $\phi(\bar{1})(\alpha) = \alpha^{-1}$.
(**Sidenote:** Thus if $o(\alpha) = n$ then $K \cong \mathbb{Z}/n\mathbb{Z}$ and $G \cong D_{2n}$ the dihedral group of order $2n$ since this was isomorphic to the same semidirect product by last week's homework. If $o(\alpha) = \infty$ then G is isomorphic to $\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ which is called the infinite dihedral group.)

2. **[Left translation of cosets.]** Given a group G and a subgroup H (not necessarily normal), G acts on the set of left cosets G/H by left translation, i.e., $w \cdot gH = wgH$. (It is easy to check that this is a well-defined action).
(a) Let $\alpha = gH \in G/H$. Show that the isotropy group G_α for this action is gHg^{-1}.
(b) If $\rho : G \to \Sigma(G/H)$ is the action homomorphism for this action, show that $ker(\rho) = \cap_{g\in G} gHg^{-1}$. Thus $Core_G(H) = \cap_{g\in G} gHg^{-1}$ is a normal subgroup of G. It is called the normal core of H in G. Show that $Core_G(H)$ is in fact the largest normal subgroup of G contained in H.
(c) Explain why $G/Core_G(H)$ is isomorphic to a subgroup of $\Sigma(G/H)$ in general. If H is a proper subgroup of G, $|G| < \infty$ and $|G|$ does not divide $|G : H|!$, conclude that $Core_G(H)$ is a nontrivial proper normal subgroup of G, i.e., $\{e\} \neq Core_G(H) \neq G$.
(d) If $|G| < \infty$, $H \leq G$ and $|G : H| = p$ where p is the smallest prime dividing $|G|$, show that $H \trianglelefteq G$.
(e) Show that any subgroup of index 2 in a group G is normal. (Here we allow G to be infinite too.)
(f) Show that A_n is the ONLY subgroup of index 2 in Σ_n for $n \geq 3$. (Hint: All 3-cycles are conjugate in Σ_n.)

3. **[No nonAbelian simple groups of order < 60.]** Recall that a simple group G is one that has $|G| > 1$ and which contains no proper nontrivial normal subgroups. In class and the notes, it was explained why no groups of order p^k, pq, p^2q where p, q distinct primes and k a nonnegative integer can

be nonAbelian simple groups.
(a) Check that using just this information, the only possible orders for a nonAbelian simple group of order < 60 are: $24, 30, 36, 40, 42, 48, 54, 56$.
(b) Show that any group of order $40, 42$ or 54 has a normal Sylow subgroup using Sylow Theory. Thus these orders cannot be the order of a nonAbelian simple group.
(c) By choosing suitable subgroups H and considering $Core_G(H)$, show that no group G of order $24, 36$ or 48 can be simple.
(d) By counting elements of certain order, show that any group of order 30 must either have a normal Sylow 3-group or a normal Sylow 5-group and hence cannot be simple.
(e) Finally show by counting elements of a certain order, that a group of order 56 has a normal Sylow subgroup. Thus there are no nonAbelian simple groups of order < 60.

4. [**The general linear group $GL_2(\mathbb{F}_p)$.**] A field $(\mathbb{F}, +, \cdot)$ is a set $\mathbb{F}$ with two binary operations addition $+$ and multiplication $\cdot$ such that:
(i) $(\mathbb{F}, +)$ is an Abelian group with identity 0.
(ii) $(\mathbb{F}, \cdot)$ is an Abelian monoid with identity 1 such that $1 \neq 0$ and such that every $x \neq 0$ is a unit.
(iii) For all $x, y, z \in \mathbb{F}$ we have $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$. [Distributivity]
Notice in a field $\mathbb{F}$, if $x \neq 0$ then $\frac{1}{x}$ exists such that $\frac{1}{x}x = 1$. We write as usual $\frac{y}{x}$ for $\frac{1}{x} \cdot y = y \cdot \frac{1}{x}$ and write $x \cdot y$ as xy. We will study fields later on more systematically, for now just note $\mathbb{C}, \mathbb{R}$ and $\mathbb{Q}$ are fields under the usual multiplication and addition. Also note that if p is a prime, $\mathbb{Z}/p\mathbb{Z}$ has properties (i) and (ii) by previous homeworks. Property (iii) holds automatically as both $+$ and $\cdot$ are induced from $\mathbb{Z}$ where distributivity holds. We will denote the field $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ by $\mathbb{F}_p$. It is called the field of p elements.
Let $Mat_n(\mathbb{F}_p)$ be the set of $n \times n$ matrices with entries in $\mathbb{F}_p$. It is easy to check that $Mat_n(\mathbb{F}_p)$ becomes a monoid (with identity $\mathbb{I}$ the usual identity matrix) under matrix multiplication $\mathbb{C} = \mathbb{A}\mathbb{B}$ given by $\mathbb{C}_{i,j} = \sum_{k=1}^{n} \mathbb{A}_{i,k}\mathbb{B}_{k,j}$. We also define for $\mathbb{A} \in Mat_n(\mathbb{F}_p)$ and $\alpha \in \mathbb{F}_p$ the scalar multiplication $\mathbb{C} = \alpha\mathbb{A}$ given by $\mathbb{C}_{i,j} = \alpha\mathbb{A}_{i,j}$. The group of units in the monoid $Mat_n(\mathbb{F}_p)$ is called the general linear group over $\mathbb{F}_p$ and denoted $GL_n(\mathbb{F}_p)$.
(a) Define $det : Mat_2(\mathbb{F}_p) \to \mathbb{F}_p$ by $det(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = ad - bc$. Check that $det : Mat_2(\mathbb{F}_p) \to (\mathbb{F}_p, \cdot)$ is a homomorphism of monoids.

(b) If $\mathbb{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(\mathbb{F}_p)$ let $adj(\mathbb{A}) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Check that for all $\mathbb{A} \in Mat_2(\mathbb{F}_p)$ we have:

$$\mathbb{A}adj(\mathbb{A}) = det(\mathbb{A})\mathbb{I} = adj(\mathbb{A})\mathbb{A}.$$

Use this to show that $GL_2(\mathbb{F}_p) = \{\mathbb{A} \in Mat_2(\mathbb{F}_p) | det(\mathbb{A}) \neq 0\}$. Compute $\mathbb{A}^{-1}$ for $\mathbb{A} = \begin{pmatrix} \bar{2} & \bar{1} \\ \bar{0} & \bar{5} \end{pmatrix} \in GL_2(\mathbb{F}_7)$. Reduce your answer so it uses entries from the standard representation of $\mathbb{F}_7$ as $\{\bar{0}, \bar{1}, \ldots, \bar{6}\}$.
(c) Show that $|GL_2(\mathbb{F}_p)| = p(p-1)^2(p+1)$. Explain why $GL_2(\mathbb{F}_{13})$ has subgroups of order $7, 9, 13$ and 32.
(d) Show that we have an epimorphism $det : GL_2(\mathbb{F}_p) \to \mathbb{F}_p^*$ where $\mathbb{F}_p^*$ is the group of nonzero elements of $\mathbb{F}_p$ under multiplication. Conclude that the kernel, which is denoted $SL_2(\mathbb{F}_p)$ and called the 2×2 special linear group over $\mathbb{F}_p$ has order $|SL_2(\mathbb{F}_p)| = p(p-1)(p+1)$.
(e) Check that $U_2(\mathbb{F}_p) = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} | b \in \mathbb{F}_p\}$ is a Sylow-p subgroup for both $GL_2(\mathbb{F}_p)$ and $SL_2(\mathbb{F}_p)$. $U_2(\mathbb{F}_p)$ is called the group of strictly upper triangular 2×2 matrices over $\mathbb{F}_p$. Calculate the normalizer of $U_2(\mathbb{F}_p)$ in $GL_2(\mathbb{F}_p)$. This normalizer is sometimes called the Borel subgroup of $GL_2(\mathbb{F}_p)$. How many Sylow-p subgroups does $GL_2(\mathbb{F}_p)$ have in general?
(f) Let $\mathbb{A} \in GL_2(\mathbb{F}_p)$ have $\mathbb{A}^p = \mathbb{I}$. Explain why there is a matrix $\mathbb{B} \in GL_2(\mathbb{F}_p)$ such that $\mathbb{B}\mathbb{A}\mathbb{B}^{-1} \in U_2(\mathbb{F}_p)$. [Hint: Use Sylow Theory!]
(g) Find the center of $GL_2(\mathbb{F}_p)$ and show that it is isomorphic to $\mathbb{F}_p^*$. Similarly show that the center or $SL_2(\mathbb{F}_p)$ is $\{\pm\mathbb{I}\}$. We define the projective general linear group $PGL_n(\mathbb{F}_p)$ as the quotient group $GL_n(\mathbb{F}_p)/Z(GL_n(\mathbb{F}_p))$. Similarly we define the projective special linear group
$PSL_n(\mathbb{F}_p) = SL_n(\mathbb{F}_p)/Z(SL_n(\mathbb{F}_p))$. Show that $|PGL_2(\mathbb{F}_p)| = p(p-1)(p+1)$ and

$$|PSL_2(\mathbb{F}_p)| = \begin{cases} \frac{p(p-1)(p+1)}{2} \text{ if } p \text{ is odd} \\ 6 \text{ if } p = 2. \end{cases}$$

(h) Show that $PSL_2(\mathbb{F}_2) \cong \Sigma_3$. By considering the left translation action of $PSL_2(\mathbb{F}_3)$ on left cosets of a Sylow-3 subgroup show that $PSL_2(\mathbb{F}_3) \cong A_4$, the alternating group on 4 letters.
(i) It turns out as we will see later, that $PSL_2(\mathbb{F}_p)$ is a nonAbelian simple group when $p \geq 5$ and one can also show that $PSL_2(\mathbb{F}_5) \cong A_5$. However show that for $p > 5$, $|PSL_2(\mathbb{F}_p)| \neq |A_m|$ for any m and hence that the family

$\{PSL_2(\mathbb{F}_p)|p > 5\}$ is a family of nonAbelian simple groups distinct from the alternating groups.

5. [**NonAbelian groups of order p^3.**] Let P be a nonAbelian p group of order p^3.
(a) Prove that $|Z(P)| = p$ and that $P/Z(P)$ is an Abelian group which is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. (Hint: If G is a group of order p^2 which isn't cyclic, find $H, K \leq G$ of order p and show that G is the direct product of H and K.)
(b) Show that the commutator subgroup P' is equal to $Z(P)$.
(c) Check that

$$U_3(\mathbb{F}_p) = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} |a, b, c \in \mathbb{F}_p\},$$

the group of strictly upper triangular 3×3 matrices over $\mathbb{F}_p$ is an example of a nonAbelian p-group of order p^3.