HW #8

7.7#1 $|G| = 2m$, m odd. (1)

G acts on itself by left multiplication, so we get a map

$$G \xrightarrow{\phi} S_{2m}$$
$$g \longmapsto l_g$$

where $l_g(g') = gg'$ for any $g' \in G$.

As $2 \mid |G|$ is a prime, Cauchy's theorem tells us there is an element $\tilde{g} \in G$ of order 2.

Note that ϕ is injective, since $h \in \ker \phi \Rightarrow$

$$l_h(g') = g' \ \forall g' \in G \Rightarrow hg' = g' \overset{\forall g' \in G}{\Rightarrow} h = e.$$

$\therefore \phi(\tilde{g})$ is an element of order 2 in S_{2m}. $\Rightarrow$ it's a product of disjoint transpositions. ~~Since~~

Moreover, since multiplication by g changes each element of G, every element appears in the transpositions defining $\phi(\tilde{g})$.

$\therefore \phi(\tilde{g})$ is a product of $\frac{2m}{2} = m$ disjoint transpositions.

Since m is odd, this means $\phi(\tilde{g}) \notin A_{2m}$. Thus

$$\phi(G) \not\subseteq A_{2m}.$$

$\therefore (\phi(G) \cap A_{2m}) \underset{\text{index 2}}{<} \phi(G)$ (2)

(because $A_{2m} < S_{2m}$ has index 2)

index 2 $\Rightarrow$ normal.

Since $\phi(G)$ is an isomorphic copy of G,

$\phi(G) \cap A_{2m}$ corresponds to a normal index 2 subgroup of G. $\square$

7.7#2 Let $H \triangleleft S_n$. Then $(H \cap A_n) \triangleleft A_n$

$\Rightarrow H \cap A_n = A_n$ or $\{e\}$ since A_n is simple.

- If $H \cap A_n = A_n$, then $H = A_n$ or S_n.
- If $H \cap A_n = \{e\}$, let $g \in H$. Then $g^2 \in H \cap A_n \Rightarrow g^2 = e$

  If $g, g' \in H$, then $gg' \in H \cap A_n \Rightarrow gg' = e \Rightarrow g' = g^{-1}$.
  ($g \neq e$, $g' \neq e$)

  $\therefore H = \langle g \rangle$ where g is a product of an odd # of disjoint transpositions.

But such a subgroup is not normal in S_n. ✗

7.7#10 Compute the commutator of $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} a & 1 \\ 0 & a^{-1} \end{pmatrix}$

for $a \neq 0$:

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} a & 1 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} a^{-1} & -1 \\ 0 & a \end{pmatrix}$$

$$= \begin{pmatrix} a^2 & a^2 \\ 0 & a^{-2} \end{pmatrix}\begin{pmatrix} a^{-2} & -1 \\ 0 & a^2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & a^4 - a^2 \\ 0 & 1 \end{pmatrix}$$

Since $|K|>3$, $\exists\, a\in K$ which is not a root of $a^4-a^2 = a^2(a-1)(a+1)$.

Done by Lemma 7.7.8.

7.7#11 Let $g\in GL_n(F)$, $|F|=q$.

Then the first column consists of a choice of number in each of n spots, except that they can't all be 0.

$\therefore q^n-1$ options for column 1st.

Inductively, there are q^n choices for column k, except it can't be in the linear span of one of the 1st $(k-1)$ colums. Since there are q^{k-1} elts in this span,

$\therefore q^n-q^{k-1}$ options for column k.

$$\therefore |GL_n(F)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$$

We compute $|SL_n(F)|$ by remembering it's the kernel of

$$GL_n(F) \xrightarrow{\det} F^\times \quad (\text{order } q-1)$$

$$\Rightarrow |SL_n(F)| = \frac{(q^n-1)\cdots(q^n-q^{n-1})}{q-1}$$

$Z(SL_n(F))$ consists of the scalar matrices of det 1. Thus $Z(SL_n(F)) = \left(\begin{array}{c}\#\text{ roots of } x^n-1=0\\ \text{in } F\end{array}\right)$

of which there are (5) $\gcd(q,n)$.

$$\therefore |PSL_n(F)| = \frac{(q^n-1)\cdots(q^n-q^{n-1})}{(q-1)\gcd(q,n)}.$$

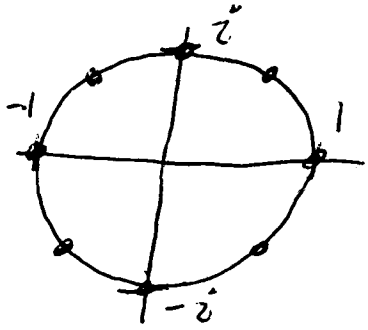
7.7 #12 By problem #11, $|F| = p^k$

$$|SL_2(F)| = \frac{(p^{2k}-1)(p^{2k}-p^k)}{p^k-1} = p^k(p^{2k}-1).$$

So the largest power of p^k dividing $SL_2(F)$ is p^k.

Easy to check $\left\{\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \middle| x \in F\right\}$ is a subgroup of $SL_2(F)$ of order p^k.

8.4 #2



(6) ~~The primitives~~

Note that

$$x^8-1 = (x-1)(x+1)(x^2+1)(x^4+1)$$

Root $+1$; Root -1; Roots $\pm i$; Roots $\frac{1}{\sqrt{2}}(\pm 1 \pm i)$ those are the prim. ones.

To show x^4+1 is irred, replace x by $(x+1)$ and use Eisenstein.

8.4 #3 Same as the midterm!

8.4 #4 The 9th roots of 1 are $e^{2\pi i k/9}$, $k=0,1,\dots,8$.

$$x^9-1 = (x-1)(x^2+x+1)(x^6+x^3+1)$$

Root $+1$; Roots $e^{2\pi i\cdot 3/9}, e^{2\pi i\cdot 6/9}$; Roots: $e^{2\pi i k/9}$ for $k \in \{1,2,4,5,7,8\}$.

An automorphism of $\mathbb{Q}(e^{2\pi i/9})$ is determined by what happens to $e^{2\pi i/9}$

Let ϕ be an automorphism of $\mathbb{Q}(e^{2\pi i/9})$ which sends $e^{2\pi i/9}$ to $e^{2\pi i\cdot 2/9}$.

Claim: ϕ has order 6.

Since $[\mathbb{Q}(e^{2\pi i/9}):\mathbb{Q}]=6$, we have $\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/9})/\mathbb{Q}) \cong \langle\phi\rangle \cong \mathbb{Z}_6$.