MATH 611 MIDTERM SOLUTIONS

1. $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G = GL_2(\mathbb{Z}/p\mathbb{Z})$

By the orbit-stabilizer theorem, $|G| = |C(x)| \cdot |Z(x)|$
(applied to the action of G on itself by conjugation)

where $Z(x) = \{ g \in G \mid g \cdot x = x \cdot g \} \leq G$ is the centralizer of x.

$$|G| = |GL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$$

$g \in Z(x)$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\Leftrightarrow$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$\Leftrightarrow \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$

$\Leftrightarrow c = 0$ & $a = d$

So $|Z(x)| = \left| \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;\middle|\; a \in (\mathbb{Z}/p\mathbb{Z})^\times, b \in \mathbb{Z}/p\mathbb{Z} \right\} \right| = p \cdot (p-1)$

$\therefore |C(x)| = |G| / |Z(x)| = p^2 - 1$ $\square$.

2. a. $G \curvearrowright X \rightsquigarrow \varphi : G \longrightarrow S_X \simeq S_n$ group homomorphism.

$g \longmapsto (x \mapsto g \cdot x)$

$\ker\varphi \trianglelefteq G$. $G/\ker\varphi \xrightarrow{\sim} \varphi(G) \leq S_X$ (first isomorphism theorem)

$\Rightarrow [G : \ker\varphi] = |G/\ker\varphi| = |\varphi(G)| \leq |S_X| = n!$

b. $|G| = 108 = 2^2 \cdot 3^3$

$s :=$ # Sylow 3-subgroups of G. Then $s \equiv 1 \bmod 3$ & $s \mid 4$ $\Rightarrow s = 1$ or 4.
(Sylow Thm 3)

If $s = 1$ then the Sylow 3-subgroup is normal. If $s = 4$, consider the action of G on the

the set X of Sylow 3-subgroups of G by conjugation $(g * H := gHg^{-1})$.

Then $G \curvearrowright X$ is transitive by Sylow Thm 2.

So, by part a, there exists a normal subgroup $K \trianglelefteq_{\neq} G$ s.t. $[G:K] \leq |X|! = 4! = 24$,

in particular $K \neq \{e\}$. So G is not simple.

3. $|G| = 175 = 5^2 \cdot 7$

$s :=$ # Sylow 5-subgroups. $s \equiv 1 \bmod 5$ & $s \mid 7 \Rightarrow s = 1$
$t :=$ # Sylow 7-subgroups. $t \equiv 1 \bmod 7$ & $t \mid 25 \Rightarrow t = 1$. (†)

Let H, K be a Sylow 5-subgroup & Sylow 7-subgroup of G.

Then $H \trianglelefteq G$ & $K \trianglelefteq G$ by (†).

Also $|H| = 5^2 \Rightarrow H \simeq \mathbb{Z}/25\mathbb{Z}$ or $(\mathbb{Z}/5\mathbb{Z})^2$
& $|K| = 7 \Rightarrow K \simeq \mathbb{Z}/7\mathbb{Z}$ in particular, H & K are abelian.

$\gcd(|H|, |K|) = 1 \overset{\text{Lagrange}}{\underset{\text{thm}}{\Rightarrow}} H \cap K = \{e\} \Rightarrow$ the map of sets $H \times K \xrightarrow{f} G$, $(h,k) \mapsto h.k$

is injective

Now $|H \times K| = |G| \Rightarrow f$ surjective, $HK = G$.

Finally $H \trianglelefteq G$, $K \trianglelefteq G$, $H \cap K = \{e\}$, & $HK = G \Rightarrow H \times K \xrightarrow[\sim]{f} G$ isom. of groups

In particular, G is abelian. □.

4. $|G| = 75 = 3 \cdot 5^2$

$s =$ # Sylow 3-subgroups. $s \equiv 1 \bmod 3$, $s \mid 25 \Rightarrow s = 1$ or 25
$t =$ # Sylow 5-subgroups $t \equiv 1 \bmod 5$, $t \mid 3 \Rightarrow t = 1$.

If $s = 1$ then, as in Q3 above $G \cong H \times K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$,
in particular G is abelian.

So, $s \neq 1$. (since G is not abelian by assumption.)

We have $H \simeq \mathbb{Z}/3\mathbb{Z}$, $H \leq G$ & $K \simeq \mathbb{Z}/25\mathbb{Z}$ or $(\mathbb{Z}/5\mathbb{Z})^2$, $K \trianglelefteq G$,

$H \cap K = \{e\}$, $HK = G$, so $G \cong K \rtimes_\varphi H$, some $\varphi : H \to \operatorname{Aut} K$ group hom.

If G contains an element of order 25, then $K \simeq \mathbb{Z}/25\mathbb{Z}$, $\operatorname{Aut} K \simeq \operatorname{Aut}(\mathbb{Z}/25\mathbb{Z})$

$$\simeq (\mathbb{Z}/25\mathbb{Z})^\times,$$

so $|\operatorname{Aut} K| = 5 \cdot (5-1) = 20$. But $|H| = 3$ & $\gcd(3,20) = 1$ $\Rightarrow$ φ is trivial

$\Rightarrow$ G is abelian $\#$ $\square$.

5. $f(x) = x+1$ is an element of G of order p^2.

Note that

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b'+ac'+b \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$$

So

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & p \cdot a & * \\ 0 & 1 & p \cdot c \\ 0 & 0 & 0 \end{pmatrix}$$

$$* = p \cdot b + ac \cdot (1+2+\dots+(p-1)) = p \cdot b + \tfrac{1}{2} p(p-1) \cdot ac$$

$$\equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mod p \quad \text{for } p \neq 2.$$

So G' does not contain an element of order p^2, & $G \not\cong G'$. $\square$.